高等学校教学用書



数 論 基 础

И. М. 維諾格拉陀夫著
裘 光 明 譯

高等教育出版社

本書系根据苏联国立技术理論書籍出版社（Государственное издательство технико-теоретической литературы）1952 年出版的維諾格拉陀夫院士（Академик И. М. Виноградов）著"数論基础"修正第六版譯出的。原書經苏联高等教育部审定为綜合大学物理数学系的教本。

本書前出第五版譯本(由商务印書館出版)曾得到北京大学閔嗣鶴教授的帮助，同时，中国科学院数学研究所所長华罗庚教授为本書写了指导性的介紹，对讀者有很大的帮助。

数 論 基 础

И. М. 維諾格拉陀夫著

裘光明譯

高等教育出版社出版
北京琉璃廠一七〇号
（北京市書刊出版業營業許可証出字第〇五四号）

京华印書局印刷　新华書店总經售

書号13010•189　開本850×1168 1/32　印張6 5/16　插頁2　字数148,000

一九五二年三月商務初版(共印7,500)

一九五六年十一月北京新一版(修訂本)

一九五六年十一月北京第一次印刷

印数0001—6,000(另平11,000)　定價(8)¥1.20(精裝本)

介紹“数論基礎”

維諾格拉陀夫院士的“数論基础”是数論領域里不可多得的一本深入淺出的好書，譯成中文，对于大学数学系的学生和爱好数論的同志都是極有帮助的。

这本書是不能粗淺地閱讀的！特别是習題部分，其中包含着十分丰富的題材，特别是維諾格拉陀夫学派的基本技术。如果讀这本書而不看不做書后的問題，就好像入宝山而空返，把这書的最重要的部分忽略了！这些問題大部分都是有根据有源流的。很多是历史上的著名問題，或是維氏自己的研究工作。他精簡地叙述了，他巧妙地安排了，使讀者逐步做去，在不知不覺中間証明了历史上有名的定理。这些高度的技巧，可能是初讀者不易發現的，同时也誠恐国内很少人能够指明給讀者关于这些問題的出处。因此我不揣冒昧地，在这里介紹一番。

在第二章的習題中，一开始就談到兩个数論上十分重要而未解决的問題：

其中一个是有名的高斯（Gauss）的圓内整点問題。所謂整点是指兩个坐标都是整数的点。設 T 是以原点为中心，r 为半徑的圓内的整点的个数。換句話說，T 就是适合

$$x^2+y^2\leqslant r^2$$

的整数(x, y)的对数。經过第二章問題 1, c, 第三章問題 6, a, 逐步地証明了

$$T=\pi r^2+O(r^{\frac{2}{3}}\ln r),$$

这是历史上有名的伏乐諾依和謝尔品斯基（Вороной-Sierpinski）的結果。而所謂高斯問題，就是要求出 $T-\pi r^2$ 的最好的上限。

这是数論中一个十分困难的問題，近若干年来經过不少数学家的努力，逐步推进，整个的历史可以概括地叙述如下：

設 θ 是最小的正整数适合下面的条件：对于任意 $\alpha>\theta$，总有

$$T=\pi r^2+O(r^{2\alpha}).$$

謝尔品斯基証明 $\theta\leqslant\frac{1}{3}$；李特伍德(Littlewood)和瓦尔非茲(Walfitz)証明 $\theta\leqslant\frac{37}{112}$；臬蘭(Nieland)更証明 $\theta\leqslant\frac{27}{82}$；梯次馬慮(Titchmarsh)用双变数方次数函数和証明 $\theta\leqslant\frac{15}{46}$。而最好的結果則是 $\theta\leqslant\frac{13}{40}$。这是罗庚在 1935 年所証明的。但是这距离大家所猜測的 $\theta\leqslant\frac{1}{4}$ 还有些距离。另一方面已經証明了 $\theta\nless\frac{1}{4}$。如何来决定这个 θ 的数値，在数論中是一个难題。

接着圓內整点問題，維氏还提出狄里虛勒(Dirichlet)的約数問題。問題是这样的：求出适合

$$xy\leqslant n,\quad x>0,\quad y>0$$

的整点的个数 T 来。經过第二章問題 1, d 和第三章問題 6, b, 可以証明

$$T=n(\ln n+2E-1)+O(n^{\frac{1}{3}}(\ln n)^2).$$

这是俄国大数学家伏乐諾依的結果。但是如果讀者把維氏的証明与伏乐諾依原来的証明比較一下，不难發現新的証法是便捷得多了。就像圓內整点問題一样，我們引进 θ，这个 θ 的历史是这样：万·德·考柏(Van der Corput)先后証明了 $\theta\leqslant\frac{33}{100}$ 和 $\theta\leqslant\frac{27}{82}$。最好的結果是迟宗陶同志的 $\theta\leqslant\frac{15}{46}$。他所用的方法是閔嗣鶴同志所提出的。

在討論上述兩个問題的过程中，維氏引入了一个十分重要的定理：(見第三章問題 5, a, 它前面一連串的問題都是帮助讀者来証明这个定理的。)

設 $A>2, k\geqslant 1$, 函数 $f(x)$ 在間隔 $Q\leqslant x\leqslant R$ 里有連續的二阶导数而且有条件

$$\frac{1}{A}\leqslant\left|f''(x)\right|\leqslant\frac{k}{A},$$

以 $\{f(x)\}$ 表示 $f(x)$ 的分数部分，则

$$\left|\sum_{Q<x\leqslant R}\{f(x)\}-\frac{1}{2}(R-Q)\right|\leqslant(2k^2(R-Q)\ln A+8kA)A^{-\frac{1}{3}}.$$

这是一个十分重要的定理(非常有用的工具)。如果把这書中所安排着的証明和万·德·考柏的相当的工作比較一下，不难發現这里要簡捷多了。

在第二章的問題里，一連串地引进了不少关于素数分布的定理。特别是問題 9, 那是历史上有名的俄国数学大师車必舍夫(Чебышев)的工作。問題 16 是茂陛烏斯(Möbius)函数的若干重要性質，而且也是与素数分布基本上相通的。問題 17, a 中引入了一个重要的方法，这方法把“爱拉托散 (Eratosthenes) 的篩子”公式化了。这与問題 23, c 联系起来，就是素数論上常用的白潤 (Brun) 方法。也就是維氏著名工作“充分大的奇数是三个素数的和”的証明中用着的一端。問題 24 是这个方法的一个簡單的应用。

第五章的問題 11 討論了所謂高斯和数。他算出形式

$$\sum_{x=0}^{m-1}e^{2\pi i\frac{Ax^2+ax}{m}}$$

的和数的絕对值。在第六章問題 11 里更把这結果推进一步。他研究了

$$\sum_{x=0}^{m-1}e^{2\pi i\frac{ax^n}{m}}$$

的絕对值的上限。在問題 15, a 里更討論了

$$\sum_{x=0}^{m-1} e^{2\pi i\frac{ax^n+bx}{m}}$$

的一个特例。由此引伸出来，我們就会發問：和式

$$\sum_{x=0}^{m-1} e^{2\pi i\frac{f(x)}{m}}, \quad f(x)=ax^n+a_1x^{n-1}+\cdots+a_n$$

的上限如何？这一个历史上的問題，已經由罗庚解决了。

不要看輕第六章的問題 13，这是維氏的重要貢献之一。从第四章問題 11 就开始了 n 次剩余的討論，而第六章問題 13 則是关于 n 次剩余分布情形的优良結果。不等式中 p 的方次数 $\frac{1}{c}$（$c = 2e^{1-\frac{1}{n}}$）是应当可以降低的。大家預測，可以用 p^ε（ε 是任意正数）来代替 $p^{\frac{1}{c}}$，但是这是一个迄未解决的問題。如果讀者能得出比 $\frac{1}{c}$ 小的数，也是值得發表的。而如果能解决这个問題，那对于数論的貢献是極大的。

同时第六章問題 12, c 也是維氏的重要貢献，罗庚曾經把它推进一步。問題 14 也是維氏自己的工作。

第五章問題 9 是苏联数学家高尔士可夫（Горшков）的結果，是普通書上所找不到的。我們知道，任意 $4m+1$ 形式的素数 p 一定是兩个平方数的和 x^2+y^2。但是究竟如何把 x 和 y 写出来？高尔士可夫回答了这个問題：

$$p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2,$$

此处 $\left(\frac{r}{p}\right)=1, \left(\frac{n}{p}\right)=-1$，而且

$$S(k)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right).$$

此外像第四章問題7引进了克魯斯脫曼(Kloostermann)和数，第五章問題10解决了沛勒(Pell)方程，第六章問題9引进了品格函数的基本性質，等等。仔細地看来，就不難發現維氏的惊人的技巧。他把这許多重要的結果分成若干問題，使讀者按步就班地，用做習題的方式，自己証明了这些結果。这是多么引人入胜的方法啊！

維諾格拉陀夫院士的全名是伊凡·馬脫維也維赤·維諾格拉陀夫(Иван Матвеевич Виноградов)，生在1892年。他是苏联科学院院士，斯泰克洛夫数学研究所所長。他还是苏联的社会主义劳动英雄，1941年获得斯大林奬金，1945年得到列宁勛章。他对数論有划时代的光輝貢献。对于用"三角和式的估值"来研究数論上的問題这一方面，在世界上是首屈一指的权威。特别是关于華林(Waring)問題的不朽的工作，以及震惊全球的关于哥尔德巴哈(Goldbach)問題的貢献。他的成就証明了社会主义的优越性，这正象征着我們的明天。

华罗庚

目　次

第五版序

許多俄罗斯数学家，諸如車必奢夫(Чебышев)，科尔欽(Коркин)，佐罗泰辽夫(Золотарёв)，馬尔可夫(Марков)，伏乐諾依(Вороной)等等，都曾研究过数論。要如道这些著名学者的古典工作的內容，可以去看狄隆涅(Б. Н. Делоне)著的“数論的彼得堡学派”那本書。

苏維埃数学家在数論領域里工作，継續着自己的先驅者的优良傳統，創造了新的强有力的方法，用来得出第一等的結果；在“苏联数学三十年”書上数論篇里，可以看到苏維埃数学家在数論領域里的成績，在那里还有着对应的文献篇目。

在我的这本書里，只是系統地叙述了大学課程范圍里数論的基础知識。書中大量的習題是为了把讀者引进数論領域的某些新观念的范圍。

这書現在的第五版与第四版有很大的不同。为了使叙述更簡單，在所有的各章里都作了很多的变动。特別大的变动是把原来的第四章和第五章合并成为新的第四章一章（因此章数减少到六个），同时关于元根的存在也有了新的更簡單的証明。

加在每章末尾的問題，都作了实質上的改編。現在問題引出的順序完全与理論材料安排的順序相配合了。引进了一些新的問題，但是問題的数目还是减去了不少。这是因为把原先独立的、然而按解决方法或者內容說是相近的問題，用 a, b, c, …記号把它們合并在一起了。重新修訂了全部的問題解答；好多地方这些解答簡化了或者用更好的代替了。在問題解答里变动得最利害的是关于 n 次剩余、非剩余和元根的分布，以及对应的三角和式的估值。

維諾格拉陀夫(И. М. Виноградов)

第一章　可除性理論

§1. 基本的概念和定理

a. 数論是研究整数的性質的。我們所説的整数不仅是自然数(正整数) 1, 2, 3, …, 还有零和負整数 −1, −2, −3, …。

通常在作理論的叙述时，我們用字母表示的只是整数。当字母所代表的不是整数时，如果意义幷不很明白，我們会作特別的声明。

兩个整数 a 和 b 的和数，差数和乘积仍然是整数，但是 a 被 b 除(假如 b 不等于零)所得到的商数，可以是整数，也可以不是整数。

b. 当 a 被 b 除得到的商数是整数时，假如把它記做 q，我們就有 $a=bq$，也就是説，a 等于 b 乘上一个整数。那末我們就説，a 被 b 除尽或者 b 除尽 a。这时 a 叫做 b 的倍数而且 b 叫做 a 的約数。b 除尽 a 这个事实，写做 $b\diagdown a$。

下面的兩个定理成立。

1. 如果 a 是 m 的倍数，m 是 b 的倍数，則 a 是 b 的倍数。

实际上，从 $a=a_1m$，$m=m_1b$ 推出 $a=a_1m_1b$，这里 a_1m_1 是整数。这就証明了定理。

2. 如果在等式 $k+l+\cdots+n=p+q+\cdots+s$ 中，除掉某一項以外，所有的項都是 b 是倍数，則这一項也是 b 的倍数。

实际上，設这一項是 k，則因为

$$l=l_1b,\quad \cdots,\quad n=n_1b,\quad p=p_1b,\quad q=q_1b,\quad \cdots,\quad s=s_1b,$$

所以

$$k=p+q+\cdots+s-l-\cdots-n=$$
$$=(p_1+q_1+\cdots+s_1-l_1-\cdots-n_1)b.$$

这就証明了定理。

c. 在一般情形下，包括 a 被 b 除尽的特殊情形在内，我們有下列定理：

每一个整数 a 可以唯一地通过正整数 b 而被表示成

$$a=bq+r;\qquad 0\leqslant r<b.$$

实际上，取 bq 等于不超过 a 的 b 的最大倍数，我們得到 a 的这种形式的一个表示式。假定还有 $a=bq_1+r_1$, $0\leqslant r_1<b$, 我們得到 $0=b(q-q_1)+(r-r_1)$，由此推出 $r-r_1$ 是 b 的倍数(b, 2)。但是由于 $|r-r_1|<b$, 所得結果只在 $r-r_1=0$, 即 $r=r_1$ 时才可能，于是还得出 $q=q_1$。

数 q 叫做 a 被 b 除的不完全商数，数 r 叫做 a 被 b 除的余数。

例子 設 $b=14$, 我們有

$$177=14\cdot 12+9,\qquad 0<9<14;$$
$$-64=14\cdot(-5)+6,\qquad 0<6<14;$$
$$154=14\cdot 11+0,\qquad 0=0<14.$$

§2. 最大公約数

a. 以后我們只討論数的正的約数。同时除尽整数 $a, b, \cdots, l$ 的每一个整数都叫做它們的公約数。公約数中最大的一个叫做最大公約数而且用符号 $(a, b, \cdots, l)$ 来表示。由于公約数的个数是有限的，最大公約数显然存在。如果 $(a, b, \cdots, l)=1$, 則 $a, b, \cdots, l$ 就說是互素的。如果数 $a, b, \cdots, l$ 中的每一个都与別的每一个互素，則 $a, b, \cdots, l$ 叫做兩兩互素的。明显地，兩兩互素的数一定也互素；而对于兩个数来說，"互素"和"兩兩互素"的概念是一样的。

例子 数 6, 10, 15, 由于(6, 10, 15) = 1, 是互素的。数 8, 13, 21, 由于 (8, 13) = (8, 21) = (13, 21) = 1, 是兩兩互素的。

b. 我們先来研究兩个数的公約数。

1. 如果 a 是 b 的倍数，則数 a 和 b 的公約数的集合与單独一个 b 的約数的集合重合；特别地，$(a, b) = b$。

实际上，数 a 和 b 的每一个公約数都是單独一个 b 的約数。反之，因为 a 是 b 的倍数，所以 (§ 1, b, 1) b 的每一个約数也都是 a 的約数，这就是說它們都是数 a 和 b 的公約数。因此数 a 和 b 的公約数的集合与單独一个 b 的約数的集合重合。而因为数 b 的最大的約数是 b 自己，所以 $(a, b) = b$。

2. 如果
$$a = bq + c,$$
則数 a 和 b 的公約数的集合与数 b 和 c 的公約数的集合重合；特别地，$(a, b) = (b, c)$。

实际上，上面所写的等式表明，数 a 和 b 的每一个公約数也除尽 c (§ 1, b, 2)，因而也是数 b 和 c 的公約数。反之，这一个等式又表明，数 b 和 c 的約数除尽 a. 因而也是数 a 和 b 的公約数。因此数 a 和 b 的公約数与数 b 和 c 的公約数是相同的一些数；特别地，这些公約数中最大的也应該相同，即 $(a, b) = (b, c)$。

c. 为了求出最大公約数，也为了获得它的最重要性質，用到下面叙述的欧儿里得(Euclid)算法。設 a 和 b 是正整数。按照 § 1, c, 我們求得一串等式

$$\left.\begin{array}{ll} a = bq_1 + r_2, & 0 < r_2 < b, \\ b = r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ r_2 = r_3 q_3 + r_4, & 0 < r_4 < r_3, \\ \cdots\cdots\cdots\cdots & \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_n q_n, & \end{array}\right\} \quad (1)$$

这串等式当我們得到一个 $r_{n+1}=0$ 时才終止。这后一点是必然的，因为 $b, r_2, r_3, \cdots$ 是遞減的正整数列，不能包括多于 b 个的正整数。

d. 自上而下来看等式組(1)，根据 b，我們可以肯定，数 a 和 b 的全体公約数与数 b 和 r_2 的全体公約数重合，也与数 r_2 和 r_3 的，数 r_3 和 r_4 的，…，数 r_{n-1} 和 r_n 的全体公約数重合，最后就与單独一个数 r_n 的全体約数重合。同时我們还有

$$(a, b)=(b, r_2)=(r_2, r_3)=\cdots=(r_{n-1}, r_n)=r_n.$$

于是我們得到了下面的一些結果。

1. 数 a 和 b 的公約数的集合与它們的最大公約数的約数集合重合。

2. 这个最大公約数等于 r_n，也就是等于欧几里得算法最后的不等于零的余数。

例子 应用欧几里得算法求(525, 231)。我們求得(輔助的計算写在右边)

525 ∣ 231 462 ∣ 2	$525=231\cdot 2+63$
231 ∣ 63 189 ∣ 3	$231=63\cdot 3+42$
63 ∣ 42 42 ∣ 1	$63=42\cdot 1+21$
42 ∣ 21 42 ∣ 2	$42=21\cdot 2$

这里最后的正余数是 $r_4=21$。所以 $(525, 231)=21$。

e. 1. 設 m 表示任意的正整数，我們有 $(am, bm)=(a, b)m$。

2. 設 δ 表示数 a 和 b 的任意公約数，我們有 $\left(\frac{a}{\delta}, \frac{b}{\delta}\right)=\frac{(a, b)}{\delta}$；特别地，我們有 $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right)=1$，这就是說，兩个数

被它們的最大公約数除所得的商数是互素的。

实际上，等式組(1)逐項地乘上 m，我們得到新的等式組，在其中代替 $a, b, r_2, \cdots, r_n$ 的是 $am, bm, r_2m, \cdots, r_nm$。所以 $(am, bm)= =r_nm$，因此命題 1 成立。

应用命題 1，我們求得

$$(a, b)=\left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right)=\left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta;$$

由此推出命題 2。

f. 1. 如果 $(a, b)=1$，則 $(ac, b)=(c, b)$。

实际上，由于 (ac, b) 除尽 ac 和 bc，按照 d, 1 它也除尽 (ac, bc)，后者根据 e, 1 等于 c；而 (ac, b) 又除尽 b，所以它也除尽 (c, b)。反之，(c, b) 除尽 ac 和 b，所以它除尽 (ac, b)。因此，(ac, b) 和 (c, b) 互相除尽，因而它們就相等了。

2. 如果 $(a, b)=1$ 而且 ac 被 b 除尽，則 c 被 b 除尽。

实际上，由于 $(a, b)=1$，我們有 $(ac, b)=(c, b)$。但是因为 ac 是 b 的倍数，所以按照 b, 1 我們有 $(ac, b)=b$，这說明 $(c, b)=b$，即 c 是 b 的倍数。

3. 如果 $a_1, a_2, \cdots, a_m$ 中的每一个与 $b_1, b_2, \cdots, b_n$ 中的每一个互素，則乘积 $a_1a_2\cdots a_m$ 也与乘积 $b_1b_2\cdots b_n$ 互素。

实际上，从定理 1，我們有

$$(a_1a_2a_3\cdots a_m, b_k)=(a_2a_3\cdots a_m, b_k)=(a_3\cdots a_m, b_k)= =\cdots=(a_m, b_k)=1,$$

然后，簡写 $a_1a_2\cdots a_m=A$，用同样的方法我們求得

$$(b_1b_2b_3\cdots b_n, A)=(b_2b_3\cdots b_n, A)= =(b_3\cdots b_n, A)=\cdots=(b_n, A)=1.$$

g. 求兩个以上的数的最大公約数的問題，可以化成求兩个数的公約数的問題。那就是說，为了求得数 $a_1, a_2, \cdots, a_n$ 的公約数，

我們写出下列的一串数:

$$(a_1, a_2)=d_2, \quad (d_2, a_3)=d_3, \quad (d_3, a_4)=d_4,$$
$$\cdots, (d_{n-1}, a_n)=d_n.$$

数 d_n 就是所有已知数的最大公約数。

实际上，根据 d, 1 数a_1 和 a_2 的全部公約数与 d_2 的全部約数重合；所以数 a_1, a_2, a_3 的全部公約数与数 d_2 和 a_3 的全部公約数重合，即与 d_3 的全部約数重合。然后我們肯定，数 a_1, a_2, a_3, a_4 的全部公約数与 d_4 的全部約数重合，等等，最后，数 $a_1, a_2, \cdots, a_n$ 的全部公約数与 d_4 的全部約数重合。而因为 d_n 的最大約数是 d_n 自己，所以它就是数 $a_1, a_2, \cdots, a_n$ 的最大公約数。

看一下上面所引的証明，我們肯定定理 d, 1 对于兩个以上的数也对。定理 e, 1 和 e, 2 也是对的，这是因为用m去乘或者用 δ 去除所有的数 $a_1, a_2, \cdots, a_n$，正像所有 $d_2, d_3, \cdots, d_n$ 都被 m 乘或者被 δ 除一样。

§ 3. 最小公倍数

a. 所有已知数的每一个整倍数都叫做它們的公倍数。最小的正的公倍数叫做最小公倍数。

b. 我們先来研究兩个数的最小公倍数。設 M 是兩个整数 a 和 b 的任意公倍数。因为它是 a 的倍数，所以$M=ak$，这里 k 是整数。但是M又是 b 的倍数，所以

$$\frac{ak}{b}$$

也应該是整数。假定 $(a, b)=d$, $a=a_1d$, $b=b_1d$，上面的整数就可以表示成$\frac{a_1k}{b_1}$，这里$(a_1, b_1)=1$ (§ 2, e, 2)。所以 k 应該被 b_1 除尽(§ 2, f, 2), $k=b_1t=\frac{b}{d}t$, 这里 t 是整数。由此

$$M=\frac{ab}{d}t.$$

反之，明显地，这种形式的每一个M既是a的倍数，也是b的倍数，因此，这是数a和b的所有公倍数的一般形狀。

这些公倍数中的最小正数，即最小公倍数，在$t=1$时得到。它就是

$$m=\frac{ab}{d}.$$

引用m，求M的公式可以改写成

$$M=mt.$$

最后这兩个等式引出下列定理：

1. 兩个数的公倍数的集合与它們的最大公約数的倍数集合重合。

2. 兩个数的最小公倍数等于它們的乘积除以它們的最大公約数。

c. 設現在需要求出兩个以上的数$a_1, a_2, \cdots, a_n$的最小公倍数。一般地用$[a, b]$表示数a和b的最小公倍数，我們写下一串数：

$$[a_1, a_2]=m_2, \quad [m_2, a_3]=m_3, \quad \cdots, \quad [m_{n-1}, a_n]=m_n.$$

用这种方法得到的m_n就是所有已知数的最小公倍数。

实际上，从 b, 1, 数a_1和a_2的全部公倍数与m_2的全部倍数重合，所以数a_1, a_2和a_3的全部公倍数与m_2和a_3的全部公倍数重合，即与m_3的全部倍数重合。然后我們肯定，数a_1, a_2, a_3, a_4的全部公倍数与m_4的全部倍数重合，等等，最后，数$a_1, a_2, \cdots, a_n$的全部公倍数与m_n的全部倍数重合。而因为m_n的最小的正倍数就是m_n自己，所以它就是数$a_1, a_2, \cdots, a_n$的最小公倍数。

从上面的証明我們看到，定理 b, 1 对于兩个以上的数也对。

此外，我們还肯定了下列定理的正确性:

兩兩互素的数的最小公倍数等于它們的乘积。

§ 4. 欧几里得算法与連分式的关系

a. 設 α 是任意的实数。用 q_1 表示不超过 α 的最大整数。在 α 不是整数时，我們有

$$\alpha = q_1 + \frac{1}{\alpha_2}, \quad \alpha_2 > 1.$$

同样地，在 $\alpha_2, \cdots, \alpha_{s-1}$ 不是整数时，我們有

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}, \quad \alpha_3 > 1;$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}, \quad \alpha_s > 1.$$

根据这个，我們得出下列分割成連分式的 α

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}}. \tag{1}$$

如果 α 是無理数，則在数列 $\alpha, \alpha_2, \cdots$ 中显然不能遇到整数，以致这种表示的步驟可以無限制地繼續下去。

如果 α 是有理数，則以后在 b 里將会看到，在数列 $\alpha, \alpha_2, \cdots$ 里一定会遇到整数，而这种表示的步驟是有尽头的。

b. 如果 α 是有理的不可約分数 $\alpha = \frac{a}{b}$，則分割 α 成連分式，就与欧几里得算法密切地有連系。实际上，我們有

$$a = bq_1 + r_2, \qquad \frac{a}{b} = q_1 + \frac{r_2}{b};$$

$$b=r_2q_2+r_3, \qquad \frac{b}{r_2}=q_2+\frac{r_3}{r_2};$$

$$r_2=r_3q_3+r_4, \qquad \frac{r_2}{r_3}=q_3+\frac{r_4}{r_3};$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-2}=r_{n-1}q_{n-1}+r_n, \qquad \frac{r_{n-2}}{r_{n-1}}=q_{n-1}+\frac{r_n}{r_{n-1}};$$

$$r_{n-1}=r_nq_n, \qquad \frac{r_{n-1}}{r_n}=q_n.$$

于是

$$\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_n}}}.$$

c. 在数 α 所分割成的連分式里出現的数 $q_1, q_2, \cdots$, 叫做不完全的商数(按照 b, 当 α 是有理数时，这就是歐几里得算法中逐次作除法所得的不完全的商数),分数

$$\delta_1=q_1, \quad \delta_2=q_1+\frac{1}{q_2}, \quad \delta_3=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}, \cdots$$

叫做近似分数。

d. 当我們注意到只要把 δ_{s-1} 里的 q_{s-1} 换成 $q_{s-1}+\frac{1}{q_s}$ 就得到 δ_s $(s>1)$ 时，我們很容易地發現了組成近似分数的非常簡單的規律。

实际上，为了統一起見，假定 $P_0=1$, $Q_0=0$, 我們可以依次把近似分数表示成下列形狀(这里等式 $\frac{A}{B}=\frac{P_s}{Q_s}$ 表示 A, B 分别由符号 P_s, Q_s 来代替):

$$\delta_1=\frac{q_1}{1}=\frac{P_1}{Q_1},$$

$$\delta_2=\frac{q_1+\dfrac{1}{q_2}}{1}=\frac{q_2q_1+1}{q_2\cdot 1+0}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{P_2}{Q_2},$$

$$\delta_3=\frac{\left(q_2+\dfrac{1}{q_3}\right)P_1+P_0}{\left(q_2+\dfrac{1}{q_3}\right)Q_1+Q_0}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{P_3}{Q_3}$$

等等，更普遍地

$$\delta_s=\frac{q_sP_{s-1}+P_{s-2}}{q_sQ_{s-1}+Q_{s-2}}=\frac{P_s}{Q_s}.$$

因此，近似分数的分子和分母可以依次按着下面的式子来計算：

$$\left.\begin{array}{l}P_s=q_sP_{s-1}+P_{s-2}\\ Q_s=q_sQ_{s-1}+Q_{s-2}\end{array}\right\}\qquad(2)$$

这些計算可以用下面的表来做：

q_s		q_1	q_2	$\cdots$			q_s	$\cdots$		q_n
P_s	1	P_1	P_2	$\cdots$	P_{s-2}	P_{s-1}	P_s	$\cdots$	P_{n-1}	a
Q_s	0	1	Q_2	$\cdots$	Q_{s-2}	Q_{s-1}	Q_s	$\cdots$	Q_{n-1}	b

例子 把数 $\frac{105}{38}$ 写成連分式。这里

105	38	2
76		
38	29	1
29		
29	9	3
27		
9	2	4
8		
2	1	2
2		

$$\frac{105}{38}=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{2}}}}$$

所以上面所説的表是

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

e. 我們来观察鄰接的近似分数的差数 $\delta_s-\delta_{s-1}$。当 $s>1$，我們有

$$\delta_s-\delta_{s-1}=\frac{P_s}{Q_s}-\frac{P_{s-1}}{Q_{s-1}}=\frac{h_s}{Q_sQ_{s-1}},$$

这里 $h_s=P_sQ_{s-1}-Q_sP_{s-1}$; 把这式子里的 P_s 和 Q_s 用(2)式来代，再化簡以后，我們得到 $h_s=-h_{s-1}$。最后这个式子結合 $h_1=q_1\cdot 0-$ $-1\cdot 1=-1$，就有 $h_s=(-1)^s$。总之，

$$P_sQ_{s-1}-Q_sP_{s-1}=(-1)^s \qquad (s>0), \qquad (3)$$

$$\delta_s-\delta_{s-1}=\frac{(-1)^s}{Q_sQ_{s-1}} \qquad (s>1). \qquad (4)$$

例子　在 d 的例子的表里，我們有

$$105\cdot 17-38\cdot 47=(-1)^5=-1.$$

f. 从(3)式推出 (P_s, Q_s) 除尽 $(-1)^s=\pm 1$(§ 1, b, 2)。

所以 $(P_s, Q_s)=1$，也就是說近似分数 $\frac{P_s}{Q_s}$ 是不可約的。

g. 設 δ_s 不等于 α (也就是除去 α 是有理数，而 δ_s 是最后的近似分数的情形)，来討論差数 $\delta_s-\alpha$ 的符号。明显地，在(1)式里用 q_s 来代替 α_s，就把 α 换成 δ_s。而从 a 看到，經过这种代替，

α_s　　减少，

α_{s-1}　　增加，

α_{s-2}　　减少，

....

$$\alpha\begin{cases} s\ \text{是奇数时减少,} \\ s\ \text{是偶数时增加。} \end{cases}$$

所以当 s 是奇数时 $\delta_s-\alpha<0$，而当 s 是偶数时 $\delta_s-\alpha>0$。因此 $\delta_s-\alpha$ 的符号与 $(-1)^s$ 相合。

h. 我們有

$$|\alpha-\delta_{s-1}|\leqslant\frac{1}{Q_sQ_{s-1}}.$$

实际上，当 $\delta_s=\alpha$ 时，这結果从(4)式得出(取等号)。当 δ_s 不等于 α 时，从(4)式和 g 里的結果，$\delta_s-\alpha$ 和 $\delta_{s-1}-\alpha$ 有不同的符号，但也可以得出这結論(取不等号)。

§5. 素数

a. 数 1 只有一个正的約数，就是 1 本身。由于这个原因，1 在自然数列里占有特殊的位置。

大于 1 的每一个整数，至少有兩个約数，就是 1 和它本身；如果它的正整数約数只有这兩个，它就叫做素数。大于 1 的整数，除掉 1 和它本身还有別的正約数的，就叫做复合数。

b. 大于一的整数的約数中間，一以外的最小約数是素数。

实际上，設整数 $a>1$，q 是它的不等于一的最小約数。如果 q 是复合数，它就有某个約数 q_1 适合条件 $1<q_1<q$；但是 a 被 q 除尽，也应該被 q_1 除尽(§1, b, 1)，这与我們对于 q 的假設矛盾。

c. 复合数 a 的不等于一的最小約数(根据 b, 它是素数)不超过 $\sqrt{a}$。

設 q 是这样的約数，那末 $a=qa_1$，$a_1\geqslant q$，兩式相乘再約去 a_1，就得出 $a\geqslant q^2$，$q\leqslant\sqrt{a}$。

d. 素数有無限多个。

只要能証明，对于任意个不同的素数 $p_1, p_2, \cdots, p_k$，总能得出

不包括在其中的新的素数，就能肯定这定理的正确性。和式 $p_1p_2\cdots p_k+1$ 的素約数就是这样的数，因为它除尽整个和式，就不可能与素数 $p_1, p_2, \cdots, p_k$ 中的任何一个相同(§ 1, b, 2)。

e. 要造出不超过已知数 N 的素数表，有一种简單的叫做爱拉托散(Eratosthenes)篩子的方法。下面讓我們来叙述这个方法。

写下数

$$1, 2, \cdots, N. \tag{1}$$

在这个数列里第一个大于一的数是 2; 它只被 1 和它自己除尽，因此它是素数。

从数列 (1) 划掉 2 以外的所有 2 的倍数(这些都是复合数)。接着 2 的第一个沒有划掉的数是 3; 它不被 2 除尽(否則它就要被划掉了)，因此 3 只被 1 和它自己除尽，所以它也是素数。

从数列 (1) 划掉 3 以外的所有 3 的倍数。接着 3 的第一个沒有划掉的数是 5; 它不被 2 也不被 3 除尽(否則它就要被划掉了)。因此，5 只被 1 和它自己除尽，所以它也是素数。

这样繼續下去。

当用所說的方法已經划掉了小于素数 p 的素数的所有倍数时，所有小于 p^2 的未划去的数目就都是素数了。实际上，小于 p^2 的每一个复合数 a，由于它的最小素約数 $\leqslant \sqrt{a} < p$，已被我們划掉了。由此推出:

1. 要划掉素数 p 的倍数，可以从 p^2 开始划起。

2. 要造出素数 $\leqslant N$ 的表，只要对于不超过 $\sqrt{N}$ 的素数的划掉它們的复合数倍数就成了。

§ 6. 素因子分解式的唯一性

a. 每一个整数 a 或者与已知素数 p 互素，或者能被 p 除尽。实际上，(a, p) 是 p 的約数，它或者等于 1，或者等于 p。在第

一种情形下，a 与 p 互素，在第二种情形下，a 被 p 除尽。

b. 如果某些因子的一个乘积能被 p 除尽，則其中至少有一个因子能被 p 除尽。

实际上，根据 a，每个因子或者与 p 互素，或者被 p 除尽。而如果所有因子都与 p 互素，則它們的乘积也与 p 互素(§2, f, 3)；所以至少有一个因子被 p 除尽。

c. 每一个大于一的整數都能分解成素因子的乘积，并且如果不考虑因子的先后次序，分解的方法还是唯一的。

实际上，設 a 是大于一的整數；用 p_1 表示它的最小的素約数，我們有 $a=p_1a_1$。如果 $a_1>1$，則用 p_2 表示它的最小的素約数，我們有 $a_1=p_2a_2$。如果 $a_2>1$，則同样地我們求得 $a_2=p_3a_3$，等等，直到引出一个等于一的 a_n 才止。那时 $a_{n-1}=p_n$。把得到的所有等式乘起来再約簡了，我們得到 a 的一个素因子分解式：

$$a=p_1p_2\cdots p_n.$$

假設对于同一个 a 还有着第二个素因子分解式 $a=q_1q_2\cdots q_s$。那末

$$p_1p_2\cdots p_n=q_1q_2\cdots q_s.$$

这等式的右边被 q_1 除尽。因此根据 b，左边至少有一个因子应該被 q_1 除尽。例如設 p_1 被 q_1 除尽（因子編号的次序是随我們的便的）；那末 $p_1=q_1$（除掉 1 以外 p_1 只被 p_1 除尽）。等式兩边約掉 $p_1=q_1$，我們有 $p_2p_3\cdots p_n=q_2q_3\cdots q_s$。对这个等式重复引用前面的論証，我們得到 $p_3\cdots p_n=q_3\cdots q_s$，等等，直到末了，等式的一边，例如左边，約掉了所有的因子时才終止。但是在同时，右边的所有因子也应該被約掉了，这是因为等式 $1=q_{n+1}\cdots q_s$ 对于大于 1 的 $q_{n+1}\cdots q_s$ 是不可能成立的。

这样一来，第二个素因子分解式与第一个完全相同。

d. 在 a 的素因子分解式中，可以有一些素因子是重复的。用

$p_1, p_2, \cdots, p_k$ 表示不同的素因子，用 $\alpha_1, \alpha_2, \cdots, \alpha_k$ 表示它們在 a 中出現的次数，我們得到所謂 a 的标准的因子分解式：

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}.$$

例子　588000 的标准分解式是：$588000=2^5\cdot3\cdot5^3\cdot7^2$。

e. 設 a 的标准分解式是 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，那末 a 的所有約数都有形式

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k};$$

$$0\leqslant\beta_1\leqslant\alpha_1,\quad 0\leqslant\beta_2\leqslant\alpha_2,\ \cdots,\quad 0\leqslant\beta_k\leqslant\alpha_k. \qquad (1)$$

实际上，設 d 除尽 a。那末 $a=dq$ (§1, b)，因此，d 的所有素約数出現在 a 的标准分解式里，其指数不小于它出現在 d 的标准分解式里的指数。所以 d 有形狀(1)。

反之，形狀(1)的每一个 d 显然除尽 a。

例子　$720=2^4\cdot3^2\cdot5$ 的所有約数有形式 $2^{\beta_1}\cdot3^{\beta_2}\cdot5^{\beta_3}$。讓 $\beta_1, \beta_2, \beta_3$ 互相独立地通过 $\beta_1=0, 1, 2, 3, 4$；$\beta_2=0, 1, 2$；$\beta_3=0, 1$。这指出那些約数是 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720。

問　題

1. 設 a 和 b 是不同时等于零的整数，而且 $d=ax_0+by_0$ 是形式 $ax+by$(x, y 是整数)的数中最小的正数。証明 $d=(a, b)$。由此引出 §2, d, 1 和 §2, e 的各个定理。再討論形式 $ax+by+\cdots+fu$ 的数来推广这个結論。

2. 証明在分母 $\leqslant Q_s$ 的所有有理分数中間，近似分数 $\delta_s=\dfrac{P_s}{Q_s}$ 最接近 α。

3. 設实数 α 已經分割成連分式，再設 N 是正整数，k 是它的十进計数法的位数，而且 n 是有条件 $Q_n\leqslant N$ 的最大整数。証明 $n\leqslant5k+1$。为了証明这个式子对于 $Q_2, Q_3, Q_4, \cdots, Q_n$ 成立，必須先

拿它們与 q_s 都等于 1 的情形比較，再拿它們与 $1, \xi, \xi^2, \cdots, \xi^{n-2}$ 比較，这里 ξ 是方程 $\xi^2=\xi+1$ 的正根。

4. 設 $\tau\geqslant 1$。具有不超过 τ 的正数分母的全部有理不可約分数，按照增加的次序排列起来，叫做与 τ 对应的法雷(Farey)級数。

a. 証明，在与 α 对应的法雷級数之中，包含着有条件 $0\leqslant\alpha\leqslant 1$ 的 α 的那一部分，可以用下列方法得到。先写下分数 $\frac{0}{1}$，$\frac{1}{1}$。如果 $2\leqslant\tau$，則在这兩个分数之間插入分数 $\frac{0+1}{1+1}=\frac{1}{2}$。然后在得到的級数 $\frac{0}{1}$，$\frac{1}{2}$，$\frac{1}{1}$ 中的每兩个鄰接的分数 $\frac{a_1}{b_1}$ 和 $\frac{c_1}{d_1}$ 之間，如果 b_1+ $+d_1\leqslant\tau$，插入分数 $\frac{a_1+c_1}{b_1+d_1}$，等等，直到不可能这样做时才止。可以預先証明，在用上述方法得到的級数中，对于任意一对鄰接的分数 $\frac{a}{b}$ 和 $\frac{c}{d}$，都有 $ad-bc=-1$。

b. 討論法雷級数来証明下面的定理：設 $\tau\geqslant 1$，那末每一个实数 α 可以表示成形式

$$\alpha=\frac{P}{Q}+\frac{\theta}{Q\tau};\quad 0<Q\leqslant\tau,\ (P,Q)=1,\quad |\theta|<1.$$

c. 利用 § 4, h 証明問題 b 的定理。

5, a. 証明形式 $4m+3$ 的素数的个数是無限的。

b. 証明形式 $6m+5$ 的素数的个数是無限的。

6. 計算不超过 N 而且在它的标准分解式里沒有 $p_1, p_2, \cdots p_k$ 以外的素約数出現的数的个数，来証明素数的个数是無限的。

7. 設 K 是正整数。証明在自然數列中有無数个連續的 M, $M+1, \cdots, M+K-1$ 不包含素数。

8. 証明在由多項式 $a_0x^n+a_1x^{n-1}+\cdots+a_n(n>0, a_0, a_1, \cdots, a_n$ 都是整数而且 $a_0>0)$ 所代表的整数中間有無数个复合数。

9, a. 証明适合不定方程

$$x^2+y^2=z^2,\quad x>0, y>0, z>0,\quad (x, y, z)=1$$

的組 x, y, z 有而且只有下列形式：x, y 和 z 分別有形式 $2uv$, u^2-v^2,和 u^2+v^2；这时 $u>v>0$, $(u, v)=1$, uv 是偶数。

b. 利用問題 a 里的定理，証明方程 $x^4+y^4=z^2$ 里的 x, y, z 沒有正整数的解答。

10. 証明定理：如果方程 $x^n+a_1x^{n-1}+\cdots+a_n=0$ ($n>0$, $a_1, \cdots, a_n$ 是整数)有有理根，則这根一定是整数。

11, a. 設 $S=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$; $n>1$。証明 S 不是整数。

b. 設 $S=\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$; $n>0$。証明 S 不是整数。

12. 設 n 是整数，$n>0$。証明，牛頓(Newton)二項式 $(a+b)^n$ 的展开式的所有系数，在而且只在 n 有形狀 2^k-1 时，才都是單数。

計 算 題

1, a. 应用欧儿里得算法求(6188, 4709)。

b. 求(81719, 52003, 33649, 30107)。

2, a. 把 $\alpha=\frac{125}{92}$ 分解成連分式，并且造出近似分数的表来(§ 4, d)。再求：α) δ_4, β)假設 $\tau=20$，把 α 表示成問題 4, b 里所說的形式。

b. 把 $\alpha=\frac{5391}{3976}$ 分解成連分式，并且造出近似分数的表来。再求：α)δ_6, β)假設 $\tau=1000$, 把 α 表示成問題 4, b 里所說的形式。

3. 造出从 0 到 1 的法雷級数（問題 4），1 不要，而且它們的分母不超过 8。

4. 造出小于 100 的素数的表来。

5, a. 求 82 798 848 的标准分解式。

b. 求 81 057 226 635 000 的标准分解式。

第二章　重要的函数

§1. 函数$[x]$和$\{x\}$

a. 在数論里函数$[x]$占着重要的地位，它对所有的实数x都有定义，表示不超过x的最大整数。这函数就叫做x的整数部分。

例子　$[7]=7$; $[2.6]=2$; $[-4.75]=-5$。

有时还会討論到函数$\{x\}=x-[x]$。这函数叫做x的分数部分。

例子　$\{7\}=0$; $\{2.6\}=0.6$; $\{-4.75\}=0.25$。

b. 为了說明前面所引的函数的用处，我們来証明定理：

在乘积$n!$里，素数p所具有的方次数等于

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots.$$

实际上，乘积$n!$中有$\left[\frac{n}{p}\right]$个因子是p的倍数，这些因子中有$\left[\frac{n}{p^2}\right]$个是$p^2$的倍数，在后面这些因子中有$\left[\frac{n}{p^3}\right]$个是$p^3$的倍数，等等。这些数目的总和就是所求的方次数，这是因为乘积$n!$的一个因子，如果是p^m的倍数而不是p^{m+1}的倍数，它作为p, p^2, p^3, $\cdots$, 直到p^m的倍数，在上述的方法中就提到了m次。

例子　在乘积$40!$里出現的3的方次数是

$$\left[\frac{40}{3}\right]+\left[\frac{40}{9}\right]+\left[\frac{40}{27}\right]=13+4+1=18.$$

§2. 对約数展开的和式

a. 数論里占特别重要的地位的是可乘函数。函数$\theta(a)$說是

可乘的，如果它适合下面的条件:

1. 函数 $\theta(a)$ 对于所有的正整数 a 都有定义，而且至少对于一个这样的 a 它不等于零。

2. 对于任何互素的正数 a_1 和 a_2 都有

$$\theta(a_1a_2)=\theta(a_1)\theta(a_2).$$

例子 不难看出，函数 $\theta(a)=a^s$ (s 是任意实数或者复数)是可乘函数。

b. 从函数 $\theta(a)$的所説的性質，特别地可以推出 $\theta(1)=1$。实际上，設 $\theta(a_0)$不等于零，那末 $\theta(a_0)=\theta(1\cdot a_0)=\theta(1)\theta(a_0)$，即 $\theta(1)=1$。除此以外，还可以得出下列重要的性質: 如果 $\theta_1(a)$ 和 $\theta_2(a)$ 都是可乘函数，則 $\theta_0(a)=\theta_1(a)\theta_2(a)$ 也是可乘函数。实际上，我們有

$$\theta_0(1)=\theta_1(1)\cdot\theta_2(1)=1.$$

并且当$(a_1, a_2)=1$ 时，我們有

$$\theta_0(a_1a_2)=\theta_1(a_1a_2)\theta_2(a_1a_2)=\theta_1(a_1)\theta_1(a_2)\theta_2(a_1)\theta_2(a_2)=$$
$$=\theta_1(a_1)\theta_2(a_1)\theta_1(a_2)\theta_2(a_2)=\theta_0(a_1)\theta_0(a_2).$$

c. 設 $\theta(a)$ 是可乘函数而 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 是 a 的标准分解式。則如果用符号 $\sum\limits_{a\diagdown d}$ 表示对于 a 的所有約数 d 展开的和式，我們有

$$\sum_{d\diagdown a}\theta(d)=\Big(1+\theta(p_1)+\theta(p_1^2)+\cdots+\theta(p_1^{\alpha_1})\Big)\cdots$$
$$\cdots\Big(1+\theta(p_k)+\theta(p_k^2)+\cdots+\theta(p_k^{\alpha_k})\Big)$$

(当 $a=1$ 时，我們認为右边等于 1)。

为了証明这个恒等式，我們脱去右边的括弧。于是我們得到下列形狀的各項之和:

$$\theta(p_1^{\beta_1})\theta(p_2^{\beta_2})\cdots\theta(p_k^{\beta_k})=\theta(p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k});$$

$$0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \cdots,\ 0\leqslant\beta_k\leqslant\alpha_k,$$

并且在展开式中沒有漏掉任何这样的一項，也沒有一項重复，而这正好是在等式左边的各項(第一章§6, e)。

d. 当 $\theta(a)=a^s$ 时，上面的恒等式变为

$$\sum_{d\diagdown a}d^s=(1+p_1^s+p_1^{2s}+\cdots+p_1^{\alpha_1 s})\cdots$$

$$\cdots(1+p_k^s+p_k^{2s}+\cdots+p_k^{\alpha_k s}).\qquad(1)$$

特别当 $s=1$ 时，(1)式左边是 a 的約数的总和 $S(a)$。化简右边，我們得到

$$S(a)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

例子

$$S(720)=S(2^4\cdot3^2\cdot5)=\frac{2^{4+1}-1}{2-1}\cdot\frac{3^{2+1}-1}{3-1}\cdot\frac{5^{1+1}-1}{5-1}=2418.$$

当 $s=0$ 时，(1)式左边是 a 的約数的个数 $\tau(a)$，我們得到

$$\tau(a)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1).$$

例子 $\tau(720)=(4+1)(2+1)(1+1)=30$。

§3. 茂陛烏斯函数

a. 茂陛烏斯(Möbius)函数 $\mu(a)$ 对于所有的正整数 a 都有定义。它由下列等式規定：$\mu(a)=0$，如果 a 被一以外的平方数除尽；$\mu(a)=(-1)^k$，如果 a 不被一以外的平方数除尽，这时 k 表示数 a 的素約数的个数；特别地，当 $a=1$ 时，我們認为 $k=0$，所以有 $\mu(1)=1$。

例子 $\mu(1)=1$, $\mu(5)=-1$, $\mu(9)=0$,

$\mu(2)=-1$, $\mu(6)=1$, $\mu(10)=1$,

$\mu(3)=-1$, $\mu(7)=-1$, $\mu(11)=-1$,

$$\mu(4)=0, \qquad \mu(8)=0, \qquad \mu(12)=0.$$

b. 設 $\theta(a)$ 是可乘函数而且

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

是 a 的标准分解式。則

$$\sum_{d\diagdown a}\mu(d)\theta(d)=(1-\theta(p_1))(1-\theta(p_2))\cdots(1-\theta(p_k)),$$

(当 $a=1$ 时,我們認为右边等于 1)。

实际上,函数 $\mu(a)$ 显然是可乘函数。所以函数 $\theta_1(a)=\mu(a)\theta(a)$ 也是可乘函数。对于函数 $\theta_1(a)$ 应用 § 2, c 的恒等式,而且根据: $\theta_1(p)=-\theta(p)$; 和对于 $s>1$, $\theta_1(p^s)=0$, 就可以肯定我們定理的正确性。

c. 特别地,假定 $\theta(a)=1$,我們从 b 得到

$$\sum_{d\diagdown a}\mu(d)\begin{cases}=0, & \text{如果}a>1,\\ =1, & \text{如果}a=1.\end{cases}$$

再假定 $\theta(d)=\frac{1}{d}$, 我們有

$$\sum_{d\diagdown a}\frac{\mu(d)}{d}\begin{cases}=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right), & \text{如果 } a>1,\\ =1, & \text{如果 } a=1.\end{cases}$$

d. 設正整数

$$\delta=\delta_1,\ \delta_2,\ \cdots,\ \delta_n$$

与任意实数或者复数 $f=f_1, f_2, \cdots, f_n$ 相对应。則如果用符号 S' 表示与等于 1 的 δ 相对应的 f 的总和, S_d 表示与倍于 d① 的 δ 相对应的 f 的总和,我們就有

$$S'=\sum\mu(d)S_d,$$

① 这里"倍于 d"意思是"d 的倍数"——譯者。

这里 d 通过至少能除尽一个 δ 的所有正整数。

实际上，根据 c 我們有

$$S'=f_1\sum_{d\diagdown\delta_1}\mu(d)+f_2\sum_{d\diagdown\delta_2}\mu(d)+\cdots+f_n\sum_{d\diagdown\delta_n}\mu(d).$$

把帶有同一个 d 值的各項归并在一起而且把 $\mu(d)$ 搬出括弧外，在括弧里我們得到的正好是与倍于 d 的 δ 相对应的那些 f 的总和，而这正好就是 S_d。

§ 4. 欧拉函数

a. 欧拉 (Euler) 函数 $\varphi(a)$ 对于所有正整数 a 都有意义，而且表示数列

$$0, 1, \cdots a-1 \tag{1}$$

里与 a 互素的数的个数。

例子
$$\varphi(1)=1,\quad \varphi(4)=2,$$
$$\varphi(2)=1,\quad \varphi(5)=4,$$
$$\varphi(3)=2,\quad \varphi(6)=2.$$

b. 設

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \tag{2}$$

是 a 的标准分解式。则

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right), \tag{3}$$

或者

$$\varphi(a)=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdots(p_k^{\alpha_k}-p_k^{\alpha_k-1}); \tag{4}$$

特別地

$$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1},\quad \varphi(p)=p-1. \tag{5}$$

实际上，我們应用 § 3, d 的定理。这时数 δ 和 f 我們这样

决定：設 x 通过数列(1)的数；对应于 x 的每个值，我們引进数 $\delta=(x,a)$ 和 $f=1$。

于是 S' 成为等于1的值 $\delta=(x,a)$ 的个数，即成为 $\varphi(a)$。而 S_d 成为倍于 d 的值 $\delta=(x,a)$ 的个数。但是 (x,a) 倍于 d 只有在 d 是 a 的約数时才成立。在这条件下 S_d 成为倍于 d 的值 x 的个数，即成为 $\frac{a}{d}$。于是我們得到

$$\varphi(a)=\sum_{d\diagdown a}\mu(d)\frac{a}{d},$$

因而根据§3, c, 就推出公式(3)，然后从(3)式根据(2)式推出公式(4)。

例子

$$\varphi(60)=60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=16;$$

$$\varphi(81)=81-27=54;$$

$$\varphi(5)=5-1=4.$$

c. 函数 $\varphi(a)$ 是可乘函数。

实际上，当 $(a_1,a_2)=1$ 时，从 b 明显地可以推出

$$\varphi(a_1a_2)=\varphi(a_1)\varphi(a_2).$$

例子 $\varphi(405)=\varphi(81)\varphi(5)=54\cdot4=216.$

d. $\sum_{d\diagdown a}\varphi(d)=a.$

为了肯定这个定理的正确性，我們应用§2, c 的恒等式，它在 $\theta(a)=\varphi(a)$ 时給出

$$\sum_{d\diagdown a}\varphi(d)=\left(1+\varphi(p_1)+\varphi(p_1^2)+\cdots+\varphi(p_1^{\alpha_1})\right)\cdots$$

$$\cdots\left(1+\varphi(p_k)+\varphi(p_k^2)+\cdots+\varphi(p_k^{\alpha_k})\right).$$

根据(5)式，右边可以改写成：

$$\left(1+(p_1-1)+(p_1^2-p_1)+\cdots+(p_1^{\alpha_1}-p_1^{\alpha_1-1})\right)\cdots$$

$$\cdots\left(1+(p_k-1)+(p_k^2-p_k)+\cdots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})\right),$$

在每个大括弧里消去同类項以后，它就等于 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=a$。

例子　假設 $a=12$，我們求得

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=$$

$$=1+1+2+2+2+4=12.$$

問　題

1, a. 設在間隔 $Q\leqslant x\leqslant R$ 里函数 $f(x)$ 是連續而且非負的。証明，和式

$$\sum_{Q<x\leqslant R}[f(x)]$$

表示在范圍：$Q<x\leqslant R,\ 0<y\leqslant f(x)$ 里的整点（有整数坐标的点）的个数。

b. 設 P 和 Q 是互素的正的奇数。証明

$$\sum_{0<x<\frac{Q}{2}}\left[\frac{P}{Q}x\right]+\sum_{0<y<\frac{P}{2}}\left[\frac{Q}{P}y\right]=\frac{P-1}{2}\cdot\frac{Q-1}{2}.$$

c. 設 $r>0$ 而 T 是在范圍 $x^2+y^2\leqslant r^2$ 里的整点的个数。証明

$$T=1+4[r]+8\sum_{0<x\leqslant\frac{r}{\sqrt{2}}}\left[\sqrt{r^2-x^2}\right]-4\left[\frac{r}{\sqrt{2}}\right]^2.$$

d. 設 $n>0$ 而且 T 是有条件 $x>0,y>0,xy\leqslant n$ 的整点的个数。証明

$$T=2\sum_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]-\left[\sqrt{n}\right]^2.$$

2. 設 $n>0$, m 是整数，$m>1$，而且 x 通过不被大于 1 的 m 次乘方数所除尽的那些正整数。証明

$$\sum_{x}\left[\sqrt[m]{\frac{n}{x}}\right]=[n].$$

3. 設 α 和 β 是这样的正数，使得下面的数

$$[\alpha x];\quad x=1,2,\cdots;\quad [\beta y];\quad y=1,2,\cdots$$

共同組成全部自然数列而且沒有重复的。証明这事实在而且只在 α 是無理数并且

$$\frac{1}{\alpha}+\frac{1}{\beta}=1$$

时才成立。

4, a. 設 $\tau\geqslant 1$, $t=[\tau]$, α 是实数而且 $x_1, x_2, \cdots, x_t$ 是数 $1,2,\cdots,t$ 的一个排列，使得数

$$0,\ \{\alpha x_1\},\ \{\alpha x_2\},\ \cdots,\ \{\alpha x_t\},\ 1$$

組成一个不减少的数列。討論这个数列中相鄰数的差数，来証明第一章問題 4, b 里的定理。

b. 設 $X, Y, \cdots, Z$ 都是不小于 1 的实数；$\alpha, \beta, \cdots, \gamma$ 也都是实数。証明有着整数 u 和不同时等于零的整数 $x, y, \cdots, z$ 存在，滿足条件：

$$|x|\leqslant X,\ |y|\leqslant Y,\ \cdots,\ |z|\leqslant Z,$$

$$(x, y, \cdots, z)=1,\ |\alpha x+\beta y+\cdots+\gamma z-u|<\frac{1}{XY\cdots Z}.$$

5. 設 α 是实数。c 是整数，$c>0$。証明

$$\left[\frac{[\alpha]}{c}\right]=\left[\frac{\alpha}{c}\right].$$

6, a. 設 $\alpha, \beta, \cdots, \lambda$ 是实数。証明

$$[\alpha+\beta+\cdots+\lambda]\geqslant[\alpha]+[\beta]+\cdots+[\lambda].$$

b. 設 $a, b, \cdots, l$ 是正整数，$a+b+\cdots+l=n$。应用 §1, b 証明

$$\frac{n!}{a!b!\cdots l!}$$

是整数。

7. 設 h 是整数，$h>0$，p 是素数，而且

$$u_s=\frac{p^{s+1}-1}{p-1}.$$

把 h 表示成形式 $h=p_m u_m+p_{m-1}u_{m-1}+\cdots+p_1u_1+p_0$，这里 u_m 是不超过 h 的最大的 u_s，$p_m u_m$ 是不超过 h 的 u_m 的最大倍数，$p_{m-1}u_{m-1}$ 是不超过 $h-p_m u_m$ 的 u_{m-1} 的最大倍数，$p_{m-2}u_{m-2}$ 是不超过 $h-p_m u_m-p_{m-1}u_{m-1}$ 的 u_{m-2} 的最大倍数，等等。証明，如果 a 是这样的数，在 $a!$ 的标准分解式里 p 的指数是 h，則有这样的 a 存在，如果而且只如果所有 $p_m, p_{m-1}, \cdots, p_1, p_0$ 都小于 p，并且在这种情形下，a 是有下列形狀的所有的数：

$$a=p_m p^{m+1}+p_{m-1}p^m+\cdots+p_1p^2+p_0p+p',\quad 0\leqslant p'<p.$$

8, a. 設在間隔 $Q\leqslant x\leqslant R$ 里函数 $f(x)$ 有連續的二阶导数。假定

$$\rho(x)=\frac{1}{2}-\{x\},\quad \sigma(x)=\int_0^x\rho(z)dz,$$

証明梭宁 (Сонин) 公式①，

$$\sum_{Q<x\leqslant R}f(x)=\int_Q^R f(x)dx+\rho(R)f(R)-\rho(Q)f(Q)-$$

$$-\sigma(R)f'(R)+\sigma(Q)f'(Q)+\int_Q^R\sigma(x)f''(x)dx.$$

① 也有叫做欧拉和数公式的——譯者。

b. 設問題 a 的条件对于充分大的 R 成立，并且 $\int\limits_{Q}^{\infty}|f''(x)|dx$ 收歛。証明

$$\sum_{Q<x\leqslant R} f(x)=C+\int^{R} f(x)dx+\rho(R)f(R)-$$

$$-\sigma(R)f'(R)-\int\limits_{R}^{\infty}\sigma(x)f''(x)dx,$$

这里 C 与 R 無关。

c. 如果 B 只取正値而且比値 $\frac{|A|}{B}$ 有上界，則我們写成 $A=$ $=O(B)$。

設 n 是整数，$n>1$。証明

$$\ln(n!)=n\ln n-n+O(\ln n).$$

9, a. 設 $n\geqslant 2$，$\Theta(z, z_0)=\sum\limits_{z_0<p\leqslant z}\ln p$，这里 p 通过素数。再設 $\Theta(z)=\Theta(z, 0)$，而且当 $x>0$ 时，

$$\psi(x)=\Theta(x)+\Theta\left(\sqrt{x}\right)+\Theta\left(\sqrt[3]{x}\right)+\cdots.$$

証明：

α) $\ln([n]!)=\psi(n)+\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)+\cdots;$

β) $\psi(n)<2n;$

γ) $\Theta\left(n, \frac{n}{2}\right)+\Theta\left(\frac{n}{3}, \frac{n}{4}\right)+\Theta\left(\frac{n}{5}, \frac{n}{6}\right)+\cdots=n\ln 2+O(\sqrt{n}).$

b. 对于 $n>2$，証明

$$\sum_{p\leqslant n}\frac{\ln p}{p}=\ln n+O(1),$$

这里 p 只通过素数。

c. 設 ε 是正的任意常数，証明在自然数列里有無数对素数 p_n, p_{n+1} 适合条件

$$p_{n+1}<p_n(1+\varepsilon).$$

d. 設 $n>2$。証明

$$\sum_{p\leqslant n}\frac{1}{p}=C+\ln\ln n+O\left(\frac{1}{\ln n}\right),$$

这里 p 通过素数而且 C 与 n 無关。

e. 設 $n>2$。証明

$$\prod_{p\leqslant n}\left(1-\frac{1}{p}\right)=\frac{C_0}{\ln n}\left(1+O\left(\frac{1}{\ln n}\right)\right),$$

这里 p 通过素数而且 C_0 与 n 無关。

10, a. 設 $\theta(a)$ 是可乘函数。証明 $\theta_1(a)=\sum_{d\backslash a}\theta(d)$ 也是可乘函数。

b. 設 $\theta(a)$ 对于所有正整数都有定义，而且 $\psi(a)=\sum_{d\backslash a}\theta(d)$ 是可乘函数。証明 $\theta(a)$ 也是可乘函数。

11. 設对于 $m>0$, $\tau_m(a)$ 表示不定方程 $x_1x_2\cdots x_m=a$ 的解答的个数 ($x_1, x_2, \cdots, x_m$ 互相独立地通过正整数)；在特別情形，明显地 $\tau_1(a)=1$, $\tau_2(a)=\tau(a)$。証明

a. $\tau_m(a)$ 是可乘函数。

b. 如果 a 的标准分解式有形式 $a=p_1p_2\cdots p_k$，則

$$\tau_m(a)=m^k.$$

c. 如果 ε 是正的任意常数，則

$$\lim_{a\to\infty}\frac{\tau_m(a)}{a^{\varepsilon}}=0.$$

d. $\sum_{0<a\leqslant n}\tau_m(a)$ 表示正整数 $x_1, x_2, \cdots, x_n$ 的不等式 $x_1x_2\cdots x_m\leqslant a$ 的解答个数。

12. 設 $R(s)$ 表示 s 的实数部分。

对于 $R(s)>1$，假定 $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$。設 $m>0$，m 是整数。証明

$$(\zeta(s))^m=\sum_{n=1}^{\infty}\frac{\tau_m(n)}{n^s}.$$

13, a. 对于 $R(s)>1$，証明

$$\zeta(s)=\prod\frac{1}{1-\frac{1}{p^s}},$$

这里 p 通过所有的素数。

b. 从調和級数的發散性出發，証明素数的个数是無限的。

c. 从 $\zeta(2)=\frac{\pi^2}{6}$ 是無理数出發，証明素数的个数是無限的。

14. 設 $\Lambda(a)=\ln p$ 对于 $a=p^l$，这里 p 是素数而 l 是正整数；$\Lambda(a)=0$ 对于其他的正整数 a。当 $R(s)>1$ 时，証明

$$\frac{\zeta'(s)}{\zeta(s)}=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

15. 設 $R(s)>1$。証明

$$\prod_p\left(1-\frac{1}{p^s}\right)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s},$$

这里 p 通过素数。

16, a. 設 $n\geqslant 1$。应用 §3, d 証明

$$1=\sum_{0<d\leqslant n}\mu(d)\left[\frac{n}{d}\right].$$

b. 設$M(z,z_0)=\sum\limits_{z_0<a\leqslant z}\mu(a)$; $M(x)=M(x,0)$。証明

α) $M(n)+M\left(\frac{n}{2}\right)+M\left(\frac{n}{3}\right)+\cdots=1,\ n\geqslant 1.$

β) $M\left(n,\frac{n}{2}\right)+M\left(\frac{n}{3},\frac{n}{4}\right)+M\left(\frac{n}{5},\frac{n}{6}\right)+\cdots=-1,\ n\geqslant 2.$

c. 設$n\geqslant 1$, l是整数，$l>1$, $T_{l,n}$是有下列条件的x的个数: $0<x\leqslant n$, x不能被大于1的l次乘方数所除尽。应用§3, d 証明

$$T_{l,n}=\sum_{d=1}^{\infty}\mu(d)\left[\frac{n}{d^l}\right].$$

17, a. 設a是整数, $a>0$,而且函数$f(x)$对于整数$x_1, x_2, \cdots, x_n$有唯一确定的值。証明

$$S'=\sum_{d\backslash a}\mu(d)S_d,$$

这里S'表示$f(x)$对于与a互素的各个x的值的展开总和，而S_d则表示$f(x)$对于倍于d的各个x的值展开的总和。

b. 設$k>1$,而且給定了下列各組

$$x_1',x_2',\cdots,x_k';\ x_1'',x_2'',\cdots,x_k'';\ \cdots;\ x_1^{(n)},x_2^{(n)},\cdots,x_k^{(n)},$$

每个組都由不全是零的整数組成。再設函数$f(x_1,x_2,\cdots,x_n)$对于这些組都有唯一确定的值。証明

$$S'=\sum\mu(d)S_d,$$

这里S'表示对于互素的数組展开的$f(x_1, x_2,\cdots, x_n)$的总和，而S_d则表示对于d的倍数組展开的$f(x_1, x_2,\cdots, x_n)$的总和。至于d则通过所有可能的正整数。

c. 設 a 是整数，$a>0$，而且函数 $F(\delta)$ 对于 a 的約数 δ 有唯一确定的值。假定

$$G(\delta)=\sum_{d\diagdown\delta}F(d),$$

証明(数字函数的轉換法則)

$$F(a)=\sum_{d\diagdown a}\mu(d)G\left(\frac{a}{d}\right).$$

d. 設正整数

$$\delta_1,\delta_2,\cdots,\delta_n$$

与不同时等于零的任意实数或者复数

$$f_1,f_2,\cdots,f_n$$

相对应。証明

$$P'=\prod P_d^{\mu(d)},$$

这里 P' 表示与等于 1 的 δ 对应的那些 f 的乘积，而 P_d 则表示与倍于 d 的 δ 对应的那些 f 的乘积。并且 d 通过所有至少能除尽一个 δ 的正整数。

18. 設 a 是整数，$a>1$，$\sigma_m(n)=1^m+2^m+\cdots+n^m$，$\psi_m(a)$ 是数列 $1,2,\cdots,a$ 中与 a 互素数的 m 次乘方的总和，$p_1,p_2,\cdots,p_k$ 是除尽 a 的所有素数。

a. 利用問題 17, a 的定理，証明

$$\psi_m(a)=\sum_{d\diagdown a}\mu(d)d^m\sigma_m\left(\frac{a}{d}\right).$$

b. 証明

$$\psi_1(a)=\frac{a}{2}\varphi(a).$$

c. 証明

$$\psi_2(a)=\left(\frac{a^2}{3}+\frac{(-1)^k}{6}p_1p_2\cdots p_k\right)\varphi(a).$$

19. 設 $z>1$, a 是整数, $a>0$, T_z 是适合条件 $0<x\leqslant z,(x,a)=1$ 的 x 的个数，而 ε 是正的任意常数。

a. 証明

$$T_z=\sum_{d\backslash a}\mu(d)\left[\frac{z}{d}\right].$$

b. 証明

$$T_z=\frac{z}{a}\varphi(a)+O(a^{\varepsilon}).$$

c. 設 $z>1$, $\pi(z)$ 是不超过 z 的素数的个数，a 是所有不超过 $\sqrt{z}$ 的素数的乘积。証明

$$\pi(z)=\pi\left(\sqrt{z}\right)-1+\sum_{d\backslash a}\mu(d)\left[\frac{z}{d}\right].$$

20. 設 $R(s)>1$, a 是整数，$a>0$。証明

$$\sum{}'\frac{1}{n^s}=\zeta(s)\prod\left(1-\frac{1}{p^s}\right),$$

这里左边的 n 通过所有与 a 互素的正整数，而右边的 p 則通过 a 的所有素約数。

21, a. k 个正整数 $x_1, x_2, \cdots, x_k$ 互相独立地取 $1, 2, \cdots, N$ 中的一个值。設 P_N 表示这样的 k 个数 $x_1, x_2, \cdots, x_k$ 互素的可能率，而 P 則表示当 $N\to\infty$ 时的可能率。应用問題 17, b 的定理；証明

$$P=(\zeta(k))^{-1}.$$

b. 設 P 是关于不可約分数 $\frac{x}{y}$ 的同样意义的可能率，(也就是在問題 a 里已知 $k=2$)，証明

$$P=\frac{6}{\pi^2}.$$

22, a. 設 $r\geqslant 2$ 而且 T 是在范圍 $x^2+y^2\leqslant r^2$ 里有互素坐标的整点 (x, y) 的个数。証明

$$T=\frac{6}{\pi}r^2+O(r\ln r).$$

b. 設 $r\geqslant 2$，而且 T 是在范圍 $x^2+y^2+z^2\leqslant r^2$ 里有互素坐标的整点 (x, y, z) 的个数。証明

$$T=\frac{4\pi}{3\zeta(3)}+O(r^2).$$

23, a. 計算 a 的所有不被大于1平方数除尽而且有 1, 2, … 个素約数的約数，来証明 § 3, c 的第一个公式。

b. 設 a 是整数，$a>1$，而 d 則通过 a 的有不多于 m 个素約数的約数；証明当 m 是偶数，$\sum\mu(d)\geqslant 0$，而当 m 是奇数，則 $\sum\mu(d)\leqslant 0$。

c. 在 § 3, d 的定理里的条件下，認为所有 f 都是非負的，而且讓 d 只通过有不多于 m 个素約数的数，来証明

$$S'\leqslant\sum\mu(d)S_d,\quad S'\geqslant\sum\mu(d)S_d$$

就看 m 是偶数还是奇数而定。

d. 在問題 17, a 的条件下，認为 $f(x)$ 的所有的値都是非負的，来証明与問題 c 里相同的不等式。再在問題 17, b 的条件下，認为 $f(x_1, x_2, \cdots, x_n)$ 的所有的値都是非負的，来証明它。

24. 設 ε 是任意常数，$0<\varepsilon<\frac{1}{6}$，$N\geqslant 2$，$r=\ln N$，$0<q\leqslant$ $\leqslant N^{1-\varepsilon}$，$0\leqslant l<q$，$(q, l)=1$，$\pi(N, q, l)$ 是适合条件 $p\leqslant N$，$p=qt+l$（t 是整数）的素数 p 的个数。証明

$$\pi(N, q, l)=O(\Delta);\ \Delta=\frac{N(qr)^{\varepsilon}}{qr}.$$

为了証明这定理，假設 $h=r^{1-\varepsilon}$。設 a 是不超过 e^h 而且不除尽 q 的所有素数的乘积。有所說条件的素数应該看作是有这些条件

并且与 a 互素的所有数的特殊情形。应該应用(有上面所說的 a 和 $m=2[2\ln r+1]$的)問題 23, d 的定理(在問題 17, a 的条件下)。

25. 設 k 是偶数，$k>0$, a 的标准分解式有形式 $a=p_1p_2\cdots p_k$，而且 d 在条件 $0<d<\sqrt{a}$ 下通过 a 的約数。証明

$$\sum_d \mu(d)=0.$$

26. 設 k 是整数，$k>0$, d 通过所有有条件 $d>0$, $\varphi(d)=k$ 的数。証明

$$\sum_d \mu(d)=0.$$

27. 利用关于 $\varphi(a)$ 的表示式，証明素数的个数是無限的。

28, a. 从确定数列 1, 2, …, a 中与 a 有同一个最大公約数 δ 的数的个数等于 $\varphi\left(\frac{a}{\delta}\right)$，来証明 § 4, d 的定理。

b. 引出关于 $\varphi(a)$ 的表示式:

α) 利用問題 10, b 的定理。

β) 利用問題 17, c 的定理。

29. 設 $R(s)>2$，証明

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}.$$

30. 設 n 是整数，$n\geqslant 2$。証明

$$\sum_{m=1}^{n}\varphi(m)=\frac{3}{\pi^2}n^2+O(n\ln n).$$

計 算 題

1, a. 求出現在 5258! 的标准分解式中的 5 的方次数 (看問

題 5)。

b. 求 125!的标准分解式。

2, a. 求 $\tau(5600)$ 和 $S(5600)$。

b. 求 $\tau(116424)$ 和 $S(116424)$。

3. 造出函数 $\mu(a)$ 对于 $a=1, 2, \cdots, 100$ 的值的表来。

4. 求 α) $\varphi(5040)$, β) $\varphi(1\,294\,700)$。

5. 造出函数 $\varphi(a)$ 对于 $a=1, 2, \cdots, 50$ 的值的表来。只能利用 § 4 的公式(5)和 § 4, c 的定理。

第三章　同余式

§1. 基本概念

a. 我們要在整数与它們被一个已知的正整数 m 除的余数的关系中来討論它們。m 叫做模。

与每个整数对应的是它被 m 除时所得到的一个确定的余数(第一章§1, c)；如果与兩个整数 a 和 b 对应的是同一个余数 r，則它們就被叫做对于模 m 同余。

b. 对于模 m 同余的数 a 和 b 写成

$$a\equiv b \pmod{m},$$

而且讀做：对于模 m，a 与 b 同余。

c. 数 a 和 b 对于模 m 的同余性，等价于：

1. a 可以表成 $a=b+mt$，这里 t 是整数。

2. $a-b$ 被 m 除尽。

实际上，从 $a\equiv b \pmod{m}$ 推出

$$a=mq+r,\quad b=mq_1+r;\quad 0\leqslant r<m,$$

由此 $$a-b=m(q-q_1),\quad a=b+mt,\quad t=q-q_1.$$

反之，从 $a=b+mt$，把 b 表成

$$b=mq_1+r,\quad 0\leqslant r<m,$$

就推出 $$a=mq+r,\quad q=q_1+t,$$

也就是 $$a\equiv b \pmod{m}.$$

所以断言 1 是对的。

从 1 直接推出断言 2。

§2. 同余式与等式相似的性質

a. 与第三个数同余的兩个数彼此同余。

从 §1, a 推出。

b. 同余式可以逐項相加。

实际上，設

$$a_1\equiv b_1 \pmod m,\quad a_2\equiv b_2 \pmod m,\ \cdots,\quad a_k\equiv b_k \pmod m. \tag{1}$$

那末(§1, c, 1)

$$a_1=b_1+mt_1,\quad a_2=b_2+mt_2,\ \cdots,\quad a_k=b_k+mt_k, \tag{2}$$

由此

$$a_1+a_2+\cdots+a_k=b_1+b_2+\cdots+b_k+m(t_1+t_2+\cdots+t_k),$$

或者(§1, c, 1)

$$a_1+a_2+\cdots+a_k\equiv b_1+b_2+\cdots+b_k \pmod m.$$

在同余式某一边的被加数可以移到另一边，只要改变它的符号就成。

实际上，把 $a+b\equiv c \pmod m$ 加到 $-b\equiv -b \pmod m$ 上，就得到 $a\equiv c-b \pmod m$。

在同余式的每一边都可以加上(或者减去)模的任意倍数。

实际上，把 $a\equiv b \pmod m$ 加到 $mk\equiv 0 \pmod m$ 上，就得到 $a+mk\equiv b \pmod m$。

c. 同余式可以逐項相乘。

实际上，再来討論同余式(1)和从它們得到的等式(2)。把(2)式逐項相乘，我們得到

$$a_1a_2\cdots a_k=b_1b_2\cdots b_k+mN,$$

这里 N 是整数。因此(§1, c, 1)

$$a_1a_2\cdots a_k\equiv b_1b_2\cdots b_k \pmod m.$$

同余式兩边可以作同一个次数的自乘。

这从前面的断言推出。

同余式两边可以乘上同一个整数。

实际上，同余式 $a\equiv b(\mathrm{mod}\ m)$ 与显然的同余式 $k\equiv k(\mathrm{mod}\ m)$ 相乘，就得到 $ak\equiv bk(\mathrm{mod}\ m)$。

d. 性質 b 和 c(同余式的加法和乘法)可以推广成下面的定理。

如果在有整系数的整有理函数 $S=\sum A_{\alpha_1,\cdots,\alpha_k}x_1^{\alpha_1}\cdots x_k^{\alpha_k}$ 中，把 $A_{\alpha_1,\cdots,\alpha_k}, x_1,\cdots,x_k$ 换成对于模 m 与它們同余的数 $B_{\alpha_1,\cdots\alpha_k}$, $y_1,\cdots,y_k$，則 S 的新的表示式对于模 m 与原先的同余。

实际上，从

$$A_{\alpha_1,\cdots,\alpha_k}\equiv B_{\alpha_1,\cdots,\alpha_k}(\mathrm{mod}\ m),$$
$$x_1\equiv y_1(\mathrm{mod}\ m),\cdots,x_k\equiv y_k(\mathrm{mod}\ m),$$

我們根据 c 得出

$$x_1^{\alpha_1}\equiv y_1^{\alpha_1}(\mathrm{mod}\ m),\cdots,x_k^{\alpha_k}\equiv y_k^{\alpha_k}(\mathrm{mod}\ \mathrm{m}),$$

$$A_{\alpha_1,\cdots,\alpha_k}x_1^{\alpha_1}\cdots x_k^{\alpha_k}\equiv B_{\alpha_1,\cdots,\alpha_k}y_1^{\alpha_1}\cdots y_k^{\alpha_k}(\mathrm{mod}\ m),$$

于是在加起来以后，我們得到

$$\sum A_{\alpha_1,\cdots,\alpha_k}x_1^{\alpha_1}\cdots x_k^{\alpha_k}\equiv\sum B_{\alpha_1,\cdots,\alpha_k}y_1^{\alpha_1}\cdots y_k^{\alpha_k}(\mathrm{mod}\ m).$$

如果

$$a\equiv b(\mathrm{mod}\ m), a_1\equiv b_1(\mathrm{mod}\ m),\cdots,a_n\equiv b_n(\mathrm{mod}\ m),$$
$$x\equiv x_1(\mathrm{mod}\ m),$$

則

$$ax^n+a_1x^{n-1}+\cdots+a_n\equiv bx^n+b_1x^{n-1}+\cdots+b_n(\mathrm{mod}\ m).$$

这命題是上述定理的特別情形。

e. 同余式两边可以被它們的公約数除，如果这公約数与模互素的話。

实际上，从 $a\equiv b \pmod{m}$, $a=a_1d$, $b=b_1d$, 推出差数 $a-b$ 等于 $(a_1-b_1)d$ 能被 m 除尽。因为 $(d, m)=1$, 所以 a_1-b_1 能被 m 除尽(第一章 § 2, f, 2), 也就是説 $a_1\equiv b_1 \pmod{m}$。

§ 3. 同余式进一步的性質

a. 同余式兩边和模可以乘上同一个整数。

实际上，从 $a\equiv b \pmod{m}$ 推出

$$a=b+mt,\quad ak=bk+mkt,$$

因此 $ak\equiv bk \pmod{mk}$。

b. 同余式兩边和模可以被它們的任意公約数除。

实际上，設

$$a\equiv b \pmod{m},\quad a=a_1d,\quad b=b_1d,\quad m=m_1d.$$

我們有

$$a=b+mt,\quad a_1d=b_1d+m_1dt,\quad a_1=b_1+m_1t,$$

因此 $a_1\equiv b_1 \pmod{m_1}$。

c. 如果同余式 $a\equiv b$ 对于几个模都成立，那末它对于与这些模的最小公倍数相等的模也成立。

实际上，从 $a\equiv b \pmod{m_1}$, $a\equiv b \pmod{m_2}$, $\cdots$, $a\equiv b \pmod{m_k}$, 推出差数 $a-b$ 能被所有的模 $m_1, m_2, \cdots, m_k$ 除尽，所以它也应該被这些模的最小公倍数 m 除尽(第一章，§ 3, c), 也就是説，$a\equiv b \pmod{m}$。

d. 如果同余式对于模 m 成立，那末它对于与 m 的任意約数相等的模 d 也成立。

实际上，从 $a\equiv b \pmod{m}$ 推出差数 $a-b$ 能被 m 除尽，所以它也应該被 m 的任意約数 d 除尽(第一章 § 1, b, 1), 也就是説，$a\equiv b \pmod{d}$。

e. 如果同余式的一边和模能被某个数除尽，則这同余式的另

外一边也能被这个数除尽。

实际上，从 $a\equiv b \pmod{m}$ 推出 $a=b+mt$，如果 a 和 m 都是 d 的倍数，則 b 也应該是 d 的倍数(第一章 §1, b, 2)。

f. 如果 $a\equiv b \pmod{m}$，那末 $(a, m)=(b, m)$。

实际上，根据第一章 §2, b, 2, 这个等式立刻从 $a=b+mt$ 推出。

§4. 完全剩余組

a. 对于模 m 同余的数組成由模 m 决定的数类。

从这个定义知道，与同一个类的所有数对应的是同一个余数 r，而且只要在式子 $mq+r$ 里讓 q 通过所有的整数，我們就得到这个类里的所有数。

对应于 r 的 m 个不同的值，我們有 m 个由模 m 决定的数类。

b. 一个类的任意数，对于同一个类的所有数而言，都叫做模 m 的剩余。当 $q=0$ 时，我們得到的剩余正好等于余数 r，叫做非負的最小剩余。

按絕对值說最小的剩余 ρ 叫做絕对的最小剩余。

明显地，当 $r<\frac{m}{2}$ 时，我們有 $\rho=r$；当 $r>\frac{m}{2}$ 时，我們有 $\rho=$ $=r-m$；最后，如果 m 是偶数而且 $r=\frac{m}{2}$，則 ρ 可以取 $\frac{m}{2}$ 和 $\frac{m}{2}-$ $-m=-\frac{m}{2}$ 两个数中的任意一个。

从每个类取一个剩余，我們得到模 m 的一个完全剩余組。最常取作完全剩余組的是全部非負的最小剩余 $0, 1, \cdots, m-1$ 或者全部絕对的最小剩余。从上面所說过的推出，絕对的最小剩余当 m 是奇数时是数列

$$-\frac{m-1}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-1}{2};$$

而当m是偶数时则是下面兩个数列的任意一个：

$$-\frac{m}{2}+1, \cdots, -1, 0, 1, \cdots, \frac{m}{2},$$

$$-\frac{m}{2}, \cdots, -1, 0, 1, \cdots, \frac{m}{2}-1.$$

c. 对于模m兩兩不同余的任意m个数，組成这个模的完全剩余組。

实际上，由于不同余的緣故，这些数屬于不同的类，而因它們的个数m正好是类的个数，所以在每个类里正好有一个数。

d. 如果$(a, m)=1$，而且x通过模m的完全剩余組，則$ax+b$（b是任意整数）也通过模m的完全剩余組。

实际上，$ax+b$的个数与x相同，即有m个。因此，根据c，只要証明与不同余的x_1和x_2对应的ax_1+b和ax_2+b对于模m也不同余就成了。

但是假設$ax_1+b \equiv ax_2+b \pmod m$，我們就能引出同余式$ax_1 \equiv ax_2 \pmod m$，于是由于$(a,m)=1$，我們就將有$x_1 \equiv x_2 \pmod m$，这与数$x_1$和$x_2$的不同余性的假設矛盾。

§ 5. 与模互素的剩余組

a. 依照§3, f，模m的同一个类里的数与模有同一个最大公約数。特别重要的是这个公約数等于一的类，即包含着与模互素的数的类。

从每个这样的类取一个剩余，我們得到与模m互素的剩余組。因此，可以取完全剩余組里与模互素的数来組成与模互素的剩余組。通常与模互素的剩余組从非負的最小剩余組$0, 1, \cdots, m-1$中分出。因为在这m个数中間，与m互素的有$\varphi(m)$个，所以与模互素的剩余組里数的个数，即包含与模互素的数的类的个数，是

$\varphi(m)$。

例子 与模 42 互素的剩余組是

$$1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$$

b. 对于模 m 兩兩不同余的任意 $\varphi(m)$ 个与模互素的数，組成一个与模 m 互素的剩余組。

实际上，由于不同余而且与模互素的緣故，这些数屬于不同的包含与模互素的数的类，而因为它們的个数 $\varphi(m)$ 正好是这种样子的类的个数，所以在每个类里正好有一个数。

c. 如果 $(a, m)=1$ 而且 x 通过与模 m 互素的剩余組，則 ax 也通过与模 m 互素的剩余組。

实际上，ax 的个数与 x 一样，即有 $\varphi(m)$ 个。因此根据 b，只要証明所有的 ax 对于模 m 兩兩不同余而且都与模互素就成了。但是第一部分在 § 4, d 里已經对于更普遍的 $ax+b$ 証明过了，而第二部分則从 $(a, m)=1$, $(x, m)=1$ 推出。

§ 6. 欧拉定理和弗尔馬定理

a. 当 $m>1$ 和 $(a,m)=1$ 时，我們有（欧拉定理）

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

实际上，如果 x 通过从非負的最小剩余得来的与模互素的剩余組

$$x=r_1, r_2, \cdots r_c; \quad c=\varphi(m),$$

則 ax 的非負的最小剩余組 $\rho_1, \rho_2, \cdots, \rho_c$ 也是这样的組，只是一般說来次序有变动罢了（§ 5, c）。

把同余式

$$ar_1 \equiv \rho_1 \pmod m, ar_2 \equiv \rho_2 \pmod m, \cdots, ar_c \equiv \rho_c \pmod m$$

逐項相乘，我們得到

$$a^c r_1 r_2 \cdots r_c \equiv \rho_1 \rho_2 \cdots \rho_c \pmod m,$$

于是从两边約掉乘积 $r_1r_2\cdots r_c=\rho_1\rho_2\cdots\rho_c$，就得出

$$a^c\equiv 1 \pmod m.$$

b. 当 p 是素数而且 a 不被 p 除尽时，我們有(弗尔馬[Fermat]定理)

$$a^{p-1}\equiv 1 \pmod p. \tag{1}$$

这定理是定理 a 当 $m=p$ 时的推論。这个定理可以給予更便利的形式。那就是說，在同余式(1)两边乘上 a，我們得到同余式

$$a^p\equiv a \pmod p,$$

它对于所有的整数 a 都正确，因为当 a 是 p 的倍数时它也成立。

問 題

1, a. 把整数写成通常的十进位数，找出能被 3, 9, 11 除尽的数的标志。

b. 把整数写成 100 进位的数，找出能被 101 除尽的数的标志。

c. 把整数写成 1000 进位的数，找出能被 37, 7, 11, 13 除尽的数的标志。

2, a. 設 $m>0$, $(a, m)=1$, b 是整数，x 和 ξ 分别通过模 m 的完全剩余組和与模互素的剩余組。証明

$$\alpha)\quad \sum_x \left\{\frac{ax+b}{m}\right\}=\frac{1}{2}(m-1),$$

$$\beta)\quad \sum_\xi \left\{\frac{a\xi}{m}\right\}=\frac{1}{2}\varphi(m).$$

b. 設 $m>0$, $(a, m)=1$; b, N, t 都是整数，$t>0$, $f(x)=\frac{ax+b}{m}$, $f(N)>0$, $f(N+mt)>0$。証明对于以直線 $x=N$, $x=N+mt$, $y=0$, $y=f(x)$ 为界的梯形，我們有

$$S=\sum\delta, \tag{1}$$

这里 S 是梯形的面积，而且右边的和式对梯形的所有整点展开：对于内点 $\delta=1$，对于頂点 $\delta=\frac{1}{4}$，而对于其他的边点 $\delta=\frac{1}{2}$。

c. 对于頂点是整点的三角形，設与問題 b 不同的是：对于頂点 $\delta=\frac{1}{6}$，証明公式(1)依然成立。

3, a. 設 $m>0$, $(a, m)=1$, $h\geqslant 0$, c 是实数，

$$S=\sum_{x=0}^{m-1}\left\{\frac{ax+\psi(x)}{m}\right\},$$

这里对于所討論的 x 的值，$\psi(x)$ 的值有条件 $c\leqslant\psi(x)\leqslant c+h$。証明

$$\left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

b. 設 M 是整数，$m>0$, $(a, m)=1$, A 和 B 都是实数，

$$A=\frac{a}{m}+\frac{\lambda}{m^2};\quad S=\sum_{x=M}^{M+m-1}\{Ax+B\}.$$

証明

$$\left|S-\frac{1}{2}m\right|\leqslant|\lambda|+\frac{1}{2}.$$

c. 設 M 是整数，$m>0$, $(a, m)=1$,

$$S=\sum_{x=M}^{M+m-1}\{f(x)\},$$

这里函数 $f(x)$ 在間隔 $M\leqslant x\leqslant M+m-1$ 里有連續的导数 $f'(x)$ 和 $f''(x)$，并且有条件

$$f'(M)=\frac{a}{m}+\frac{\theta}{m^2};\quad (a, m)=1;\quad |\theta|<1,\quad \frac{1}{A}\leqslant\left|f''(x)\right|\leqslant\frac{k}{A},$$

这里

$$1\leqslant m\leqslant\tau,\quad \tau=A^{\frac{1}{3}},\quad A\geqslant 2,\quad k\geqslant 1.$$

証明
$$\left|S-\frac{1}{2}m\right|<\frac{k+3}{2}.$$

4. 設在把無理数 A 分割成連分式时，所有不完全商数都是有界的。再設 M 是整数，m 是整数，$m>0$，B 是实数，証明
$$\sum_{x=M}^{M+m-1}\{Ax+B\}=\frac{1}{2}m+O(\ln m).$$

5, a. 設 $A>2$, $k\geqslant 1$，而且函数 $f(x)$ 在間隔 $Q\leqslant x\leqslant R$ 里有連續的二阶导数，适合条件
$$\frac{1}{A}\leqslant\left|f''(x)\right|\leqslant\frac{k}{A}.$$

証明
$$\sum_{Q<x\leqslant R}\{f(x)\}=\frac{1}{2}(R-Q)+\theta\Delta;\quad |\theta|<1,$$
$$\Delta=(2k^2(R-Q)\ln A+8kA)A^{-\frac{1}{3}}.$$

b. 設 $0<\sigma\leqslant 1$，Q 和 R 都是整数。在問題 a 的条件下，証明当 $x=Q+1, \cdots, R$ 时，适合条件 $0\leqslant\{f(x)\}<\sigma$ 的分数 $\{f(x)\}$ 的个数 $\psi(\sigma)$ 可以用下列公式来表示
$$\psi(\sigma)=\sigma(R-Q)+\theta'\cdot 2\Delta;\quad |\theta'|<1.$$

6, a. 設 T 是在范圍 $x^2+y^2\leqslant r^2$ $(r\geqslant 2)$ 里的整点 (x, y) 的个数。証明
$$T=\pi r^2+O\left(r^{\frac{2}{3}}\ln r\right).$$

b. 設 n 是整数，$n>2$，E 是欧拉常数①。証明
$$\tau(1)+\tau(2)+\cdots+\tau(n)=n(\ln n+2E-1)+O\left(n^{\frac{1}{3}}(\ln n)^2\right).$$

---

① 欧拉常数 $E=\lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\ln n\right)$——譯者。

7. n 个正整数，每一个都用 2 的不同乘方的和数来表示，組成一个組，如果对于任何非負的 s, 有 2^s 項的数的个数都是偶数，这个組就叫做規則的；而如果对于某一个 s, 这样的数的个数是奇数，則这个組就叫做不規則的。

証明，不規則的組能从适当地减少，或者完全取消其中的某一个数而变成規則的；而規則的組在减少，或者完全取消其中的任意一个数以后，就变成不規則的。

8, a. 証明，当 $x_n, x_{n-1}, \cdots, x_1, x_0$ 互相独立地通过 $-1, 0, 1$ 时，

$$3^n x_n + 3^{n-1} x_{n-1} + \cdots + 3x_1 + x_0。$$

表示所有下面的数

$$-H, \cdots, -1, 0, 1, \cdots, H; \ H = \frac{3^{n+1}-1}{3-1},$$

并且每个数都只有唯一的表示法。

b. 設 $m_1, m_2, \cdots, m_k$ 是兩兩互素的正整数。利用 § 4, c, 証明模 $m_1 m_2 \cdots m_k$ 的完全剩余組可以用下面的式子表示：

$$x_1 + m_1 x_2 + m_1 m_2 x_3 + \cdots + m_1 m_2 \cdots m_{k-1} x_k,$$

这里 $x_1, x_2, \cdots, x_k$ 分別通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余組。

9. 設 $m_1, m_2, \cdots, m_k$ 兩兩互素而且

$$m_1 m_2 \cdots m_k = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k.$$

a. 应用 § 4, c, 証明模 $m_1 m_2 \cdots m_k$ 的完全剩余組可以用下面的式子表示：

$$M_1 x_1 + M_2 x_2 + \cdots + M_k x_k,$$

这里 $x_1, x_2, \cdots, x_k$ 通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余組。

b. 应用 § 5, b 和第二章 § 4, c, 証明与模 $m_1 m_2 \cdots m_k$ 互素的剩余組可以用下面的式子表示：

$$M_1 x_1 + M_2 x_2 + \cdots + M_k x_k,$$

这里 $x_1, x_2, \cdots, x_k$ 通过与模 $m_1, m_2, \cdots, m_k$ 互素的剩余組。

c. 不用第二章 § 4, c 的第一个定理，証明問題 b 的定理，那时前一个定理就是后一个定理的推論了。

d. 用初等的方法求 $\varphi(p^{\alpha})$ 的表示式。再利用第二章 § 4, c 的等式，引出关于 $\varphi(a)$ 的已知表示式来。

10. 設 $m_1, m_2, \cdots, m_k$ 兩兩互素而且都大于 1, $m=m_1m_2\cdots m_k$, $m_sM_s=m$。

a. 設 $x_1, x_2, \cdots, x_k, x$ 和 $\xi_1, \xi_2, \cdots, \xi_k, \xi$ 分別通过模 $m_1, m_2, \cdots, m_k, m$ 的完全剩余組和与模互素的剩余組。証明分数

$$\left\{\frac{x_1}{m_1}+\frac{x_2}{m_2}+\cdots+\frac{x_k}{m_k}\right\}$$

与分数 $\left\{\frac{x}{m}\right\}$ 相等，而 $\left\{\frac{\xi_1}{m_1}+\frac{\xi_2}{m_2}+\cdots+\frac{\xi_k}{m_k}\right\}$ 則与 $\left\{\frac{\xi}{m}\right\}$ 相等。

b. 設給了 $r(r\geqslant 1)$ 个变数 $x, \cdots, w$ 的 k 个有整系数的有理函数：

$$f_s(x, \cdots, w)=\sum_{\alpha, \cdots, \delta} c^{(s)}_{\alpha, \cdots, \delta} x^{\alpha}\cdots w^{\delta};\quad s=1, \cdots, k.$$

再設当 $x_s, \cdots, w_s$ 和 $\xi_s, \cdots, \omega_s$ 分別通过模 m_s 的完全剩余組和与模互素的剩余組，而 $x, \cdots, w$ 和 $\xi, \cdots, \omega$ 則分別通过模 m 的完全剩余組和与模互素的剩余組时，

$$f(x, \cdots, w)=\sum_{\alpha, \cdots, \delta} c_{\alpha, \cdots, \delta} x^{\alpha}\cdots w^{\delta};\quad c_{\alpha, \cdots, \delta}=\sum_{s=1}^{k} M_s c^{(s)}_{\alpha, \cdots, \delta}.$$

証明 $\left\{\frac{f_1(x_1, \cdots, w_1)}{m_1}+\cdots+\frac{f_k(x_k, \cdots, w_k)}{m_k}\right\}$ 与 $\left\{\frac{f(x, \cdots, w)}{m}\right\}$ 相等，

而 $\left\{\frac{f_1(\xi_1, \cdots, \omega_1)}{m_1}+\cdots+\frac{f_k(\xi_k, \cdots, \omega_k)}{m_k}\right\}$ 則与 $\left\{\frac{f(\xi, \cdots, \omega)}{m}\right\}$ 相等

(这是問題 a 的定理的推广)。

11, a. 設 m 是整数，$m>0$, a 是整数，x 通过模 m 的完全剩余組。証明

$$\sum e^{2\pi i\frac{ax}{m}}=\begin{cases}m, \text{如果 } a \text{ 是 } m \text{ 的倍数},\\ 0, \text{其他情形。}\end{cases}$$

b. 設 α 是实数，M 是整数，P 是整数，$P>0$。符号 (α) 表示 α 与离 α 最近的整数的差数（α 到最近的整数的距离）。証明

$$\left|\sum_{x=M}^{M+P-1} e^{2\pi i\alpha x}\right|\leqslant \min\left(P, \frac{1}{h(\alpha)}\right);\quad h\geqslant\begin{cases}2, \text{所有情形},\\ 3, \text{当 } (\alpha)\leqslant\frac{1}{6}\text{。}\end{cases}$$

c. 設 m 是整数，$m>1$，函数 $M(a)$ 和 $P(a)$ 对于 $a=1, 2, \cdots, m-1$ 有整数值而且有条件 $P(a)>0$。証明

$$\sum_{a=1}^{m-1}\left|\sum_{x=M(a)}^{M(a)+P(a)-1} e^{2\pi i\frac{a}{m}x}\right|<\begin{cases}m\ln m-\frac{m}{3}\ln\left(2\left[\frac{m}{6}\right]+1\right),\\ m\ln m-\frac{m}{2}, \text{ 当 } m\geqslant 12 \text{ 时},\\ m\ln m-m, \text{ 当 } m\geqslant 60 \text{ 时。}\end{cases}$$

12, a. 設 m 是整数，$m>0$，ξ 通过与 m 互素的剩余組。証明

$$\mu(m)=\sum_{\xi} e^{2\pi i\frac{\xi}{m}}.$$

b. 利用問題 a 的定理，証明第二章 § 3, c 的第一个定理。（参看第二章問題 28, a 的解）

c. 利用第二章問題 17, a 的定理，引出問題 a 的定理。

d. 設

$$f(x, \cdots, w)=\sum_{\alpha, \cdots, \delta} c_{\alpha, \cdots, \delta}\, x^{\alpha}\cdots w^{\delta}$$

是 r 个变数 $x, \cdots, w$ $(r\geqslant 1)$ 的有整系数的有理函数，a 是整数，m 是整数，$m>0$；$x, \cdots, w$ 和 $\xi, \cdots, \omega$ 分别通过模 m 的完全剩余組和与模互素的剩余組。引进記号

$$S_{a,m}=\sum_{x}\cdots\sum_{w}e^{2\pi i\frac{af(x,\cdots,w)}{m}},\quad S'_{a,m}=\sum_{\xi}\cdots\sum_{\omega}e^{2\pi i\frac{af(\xi,\cdots,\omega)}{m}}.$$

再設 $m=m_1\cdots m_k$, $m_1,\cdots,m_k$ 兩兩互素，都大于 1，而且設 $m=m_sM_s$。証明

$$S_{a_1,m_1}\cdots S_{a_k,m_k}=S_{M_1a_1+\cdots+M_ka_k,m}$$

$$S'_{a_1,m_1}\cdots S'_{a_k,m_k}=S'_{M_1a_1+\cdots+M_ka_k,m}.$$

e. 在問題 d 的記号下，假定

$$A(m)=m^{-r}\sum_{a}S_{a,m},\ A'(m)=m^{-r}\sum_{a}S'_{a,m},$$

这里 a 通过与模 m 互素的剩余組。証明

$$A(m_1)\cdots A(m_k)=A(m),\quad A'(m_1)\cdots A'(m_k)=A'(m).$$

13, a. 証明

$$\varphi(a)=\sum_{n=0}^{a-1}\prod_{p}\left(1-\frac{1}{p}\sum_{x=0}^{p-1}e^{2\pi i\frac{nx}{p}}\right),$$

这里 p 通过 a 的素約数。

b. 从問題 a 的恒等式推出 $\varphi(a)$的已知表示式。

14. 証明

$$\tau(a)=\lim_{\varepsilon\to 0}2\varepsilon\sum_{0<x<\sqrt{a}}\sum_{k=1}^{\infty}\frac{e^{2\pi i\frac{ak}{x}}}{k^{1+\varepsilon}}+\delta,$$

这里 $\delta=0$ 或者 $\delta=1$，就看 a 是不是平方数而定。

15, a. 設 p 是素数而且 $h_1,h_2,\cdots,h_a$ 都是整数。証明

$$(h_1+h_2+\cdots+h_a)^p\equiv h_1^p+h_2^p+\cdots+h_a^p\pmod p。$$

b. 从問題 a 的定理引出弗尔馬定理。

c. 从弗尔馬定理引出欧拉定理。

計 算 題

1. a. 求$(12371^{56}+34)^{28}$被111除所得的余数。

b. $2^{1093}-2$能被1093^2除尽嗎?

2. a. 应用問題1的可除性标志,求244 943 325的标准分解式。

b. 求282 321 246 671 737的标准分解式。

第四章　一个未知数的同余式

§1. 基本概念

我們現在的任务是研究下列形狀的同余式:

$$f(x)\equiv 0 \pmod m;\ f(x)=ax^n+a_1x^{n-1}+\cdots+a_n. \qquad (1)$$

如果 a 不被 m 除尽，則 n 叫做同余式的次数。

解同余式也就是找出适合同余式的所有 x 來。被 x 的同一些值所适合的兩个同余式叫做等价的。

如果同余式(1)被某个 $x=x_1$ 所适合，則根据第三章 §2, d, 同一个同余式也被对于模 m 与 x_1 同余的所有数 $x\equiv x_1 \pmod m$ 所适合。整个这个数类被認为是一个解答。在这种約定下，同余式(1)有几个解答，就看在完全剩余組里适合它的剩余有几个。

例子　同余式

$$x^5+x+1\equiv 0 \pmod 7$$

被模 7 的完全剩余組 0, 1, 2, 3, 4, 5, 6 里的兩个数 $x=2$ 和 $x=4$ 所适合。所以这个同余式有兩个解答:

$$x\equiv 2 \pmod 7,\ x\equiv 4 \pmod 7.$$

§2. 一次同余式

a. 一次同余式在把自由項移到左边(取相反的正負号)以后，可以化成

$$ax\equiv b \pmod m. \qquad (1)$$

b. 在进行研究解答个数的問題时，我們先用条件 $(a, m)=1$ 来限制同余式。根据 §1, 我們的同余式有几个解答，也就是完全剩余組里有几个剩余适合它。但是当 x 通过模 m 的完全剩余組

时，ax 也通过完全剩余組(第三章 § 4, d)。因此，特別地，对于 x 从完全剩余組取得的一个而且只一个值，ax 与 b 同余。总之，当 $(a, m)=1$ 时，同余式(1)有一个解。

c. 現在設 $(a, m)=d>1$。那末，要同余式(1)有解答，必須 b 被 d 除尽(第三章 § 3, c)，否則就沒有任何整数 x 能使同余式(1)成立。假如 b 是 d 的倍数，我們讓 $a=a_1d$, $b=b_1d$, $m=m_1d$。于是同余式 (1) 就等价于約去 d 以后的同余式 $a_1x\equiv b_1 \pmod{m_1}$, 在其中已經有 $(a_1, m_1)=1$, 因而它有对于模 m_1 的一个解答。設 x_1 是这个解答对于模 m_1 的非負的最小剩余，那末組成这个解答的所有数 x, 可以在下列式子里求得:

$$x\equiv x_1 \pmod{m_1}. \qquad (2)$$

对于模 m 說，(2)式里的数不只組成一个解答，而是更多些，解答的个数与在模 m 的最小剩余組 $0, 1, 2, \cdots, m-1$ 里找到的(2)式里数的个数相同。而在那里面的有下面几个(2)式里的数:

$$x_1,\ x_1+m_1,\ x_1+2m_1,\ \cdots,\ x_1+(d-1)m_1,$$

即一共有 d 个(2)式的数，因此同余式(1)有 d 个解。

d. 以上兩段所証明的所有結果，可以归幷成下列定理:

設 $(a, m)=d$。当 b 不被 d 除尽时，同余式 $ax\equiv b \pmod{m}$ 不能成立。当 b 是 d 的倍数时，这同余式有 d 个解。

e. 現在来探求同余式(1)的解答。我們只想指出基于連分式理論的一种方法，幷且只要限于 $(a, m)=1$ 的情形就够了。

把比値 $m:a$ 分割成連分式

$$\frac{m}{a}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cdots+\cfrac{1}{q_n}}}$$

来討論兩个鄰接的近似分数:

$$\frac{P_{n-1}}{Q_{n-1}},\quad \frac{P_n}{Q_n}=\frac{m}{a},$$

按照連分式的性質(第一章 § 4, e), 我們有

$$mQ_{n-1}-aP_{n-1}=(-1)^n,$$

$$aP_{n-1}\equiv(-1)^{n-1}(\bmod m),$$

$$a\cdot(-1)^{n-1}P_{n-1}b\equiv b(\bmod m).$$

所以我們的同余式有解答

$$x\equiv(-1)^{n-1}P_{n-1}b(\bmod m),$$

要求出这个解答, 只要按照第一章 § 4, d 里所說的方法来計算 P_{n-1}。

例子 解同余式

$$111x\equiv75(\bmod 321).\tag{3}$$

这里(111, 321)=3, 并且 75 是 3 的倍数。所以这同余式有三个解答。

用 3 去除同余式兩边和模, 我們得到同余式

$$37x\equiv25(\bmod 107),\tag{4}$$

这是我們应該先解的, 我們有

107 | 37
74 | 2
37 | 33
33 | 1
33 | 4
32 | 8
4 | 1
4 | 4

q		2	1	8	4
P_s	1	2	3	26	107

这說明在已知情形里, $n=4$, $P_{n-1}=26$, $b=25$, 所以同余式(4)

的解答是

$$x \equiv -26 \cdot 25 \equiv 99 \pmod{107}.$$

由此，同余式(3)的解答就是：

$$x \equiv 99;\ 99+107;\ 99+2\cdot 107 \pmod{321},$$

也就是 $$x \equiv 99;\ 206;\ 313 \pmod{321}.$$

§3. 一次同余式組

a. 我們只討論最簡單的同余式組：

$$x \equiv b_1 \pmod{m_1},\ x \equiv b_2 \pmod{m_2},\ \cdots,\ x \equiv b_k \pmod{m_k}, \qquad (1)$$

它們有一个未知数，而且有不同的兩兩互素的模。

b. 解同余式組(1)，也就是找出所有适合它們的 x，可以应用下面的定理：

設数 M_s 和 M'_s 由下面的条件定出：

$$m_1 m_2 \cdots m_k = M_s m_s,\ M_s M'_s \equiv 1 \pmod{m_s},$$

而且設

$$x_0 = M_1 M'_1 b_1 + M_2 M'_2 b_2 + \cdots + M_k M'_k b_k.$$

那末适合組(1)的全部 x 可以由下面的同余式定出：

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}. \qquad (2)$$

实际上，由于所有的 M_j（除去 M_s）都能被 m_s 除尽，对于任意的 $s=1, 2, \cdots, k$，我們有

$$x_0 \equiv M_s M'_s b_s \equiv b_s \pmod{m_s},$$

这样，$x=x_0$ 就适合組(1)了。由此直接推出組(1)与組

$$x \equiv x_0 \pmod{m_1},\ x \equiv x_0 \pmod{m_2},\ \cdots,\ x \equiv x_0 \pmod{m_k} \qquad (3)$$

等价（也就是說組(1)和(3)被 x 的同一些値所适合）。而根据第三章§3, c 和第三章§3, d 的定理，組(3)被而且只被适合同余式(2)的那些 x 値所适合。

c. 如果 $b_1, b_2, \cdots, b_k$ 互相独立地通过模 $m_1, m_2, \cdots, m_k$ 的完全

剩余組，則 x_0 通过模 $m_1m_2\cdots m_k$ 的完全剩余組。

实际上，x_0 所通过的 $m_1m_2\cdots m_k$ 个値，根据第三章 § 1, d, 对于模 $m_1m_2\cdots m_k$ 是不同余的。

d. 例子 解同余式組

$$x\equiv b_1 \pmod 4,\quad x\equiv b_2 \pmod 5,\quad x\equiv b_3 \pmod 7.$$

这里 $4\cdot5\cdot7=4\cdot35=5\cdot28=7\cdot20$, 并且

$$35\cdot3\equiv1 \pmod 4,\ 28\cdot2\equiv1 \pmod 5,\ 20\cdot6\equiv1 \pmod 7.$$

所以

$$x_0=35\cdot3\,b_1+28\cdot2\,b_2+20\cdot6\,b_3=105\,b_1+56\,b_2+120\,b_3,$$

因此适合已知組的 x 的全部値可以表示成

$$x\equiv105\,b_1+56\,b_2+120\,b_3 \pmod{140}.$$

例如适合組

$$x\equiv1 \pmod 4,\ x\equiv3 \pmod 5,\ x\equiv2 \pmod 7$$

的 x 的全部値是

$$x\equiv105\cdot1+56\cdot3+120\cdot2\equiv93 \pmod{140}.$$

而适合組

$$x\equiv3 \pmod 4,\ x\equiv2 \pmod 5,\ x\equiv6 \pmod 7$$

的 x 的全部値是

$$x\equiv105\cdot3+56\cdot2+120\cdot6\equiv27 \pmod{140}.$$

§ 4. 素数模的任意次同余式

a. 設 p 是素数，我們来証明关于下面形式的同余式的普遍定理：

$$f(x)\equiv0 \pmod p;\ f(x)=ax^n+a_1x^{n-1}+\cdots+a_n. \qquad (1)$$

b. 同余式(1)与一个次数不高于 $p-1$ 的同余式等价。

实际上，用 x^p-x 去除 $f(x)$，我們有

$$f(x)=(x^p-x)Q(x)+R(x),$$

这里 $R(x)$ 的次数不高于 $p-1$。而因为 $x^p-x\equiv0\pmod p$，所以 $f(x)\equiv R(x)\pmod p$，于是就推出所說的定理。

c. 如果同余式(1)有多于 n 个的解答，則 $f(x)$ 的所有系数都是 p 的倍数。

实际上，設同余式(1)至少有 $n+1$ 个解答。用 $x_1, x_2, \cdots, x_n, x_{n+1}$ 来表示这些解答的剩余，我們可以把 $f(x)$ 表示成

$$\begin{aligned}f(x)=&a(x-x_1)(x-x_2)\cdots(x-x_{n-2})(x-x_{n-1})(x-x_n)+\\&+b(x-x_1)(x-x_2)\cdots(x-x_{n-2})(x-x_{n-1})+\\&+c(x-x_1)(x-x_2)\cdots(x-x_{n-2})+\\&+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots+\\&+k(x-x_1)(x-x_2)+\\&+l(x-x_1)\\&+m.\end{aligned}\tag{2}$$

为了这个目的，把(2)式右边各項展开(去括弧)成多項式，这样来取 b，使得多項式前两項中 x^{n-1} 的系数的和等于 a_1；知道了 b，这样来取 c，使得多項式前三項中 x^{n-2} 的系数的和等于 a_2；等等。

在(2)式中依次讓 $x=x_1, x_2, \cdots, x_n, x_{n+1}$，可以肯定所有 $m, l, k, \cdots, c, b, a$ 都是 p 的倍数。这說明所有 $a, a_1, \cdots, a_n$ (作为 p 的倍数之和)也都是 p 的倍数。

d. 对于素数 p，下面的同余式成立(威尔逊[Wilson]定理)：

$$1\cdot2\cdots(p-1)+1\equiv0\pmod p.\tag{3}$$

实际上，当 $p=2$ 时，定理是显然的。而如果 $p>2$，則我們来看一下同余式

$$(x-1)(x-2)\cdots(x-(p-1))-(x^{p-1}-1)\equiv0\pmod p;$$

它的次数不高于 $p-2$ 却有 $p-1$ 个解答，那就是有剩余 $1, 2, \cdots, p-1$ 的解答。因此，从 c 的定理，它的所有系数都是 p 的倍数；特别地，正好等于同余式(3)左边的它的自由項能被 p 除尽。

例子 我們有 $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6+1=721\equiv 0 \pmod 7$.

§ 5. 复合数模的任意次同余式

a. 如果 $m_1, m_2, \cdots, m_k$ 兩兩互素，則同余式

$$f(x)\equiv 0 \pmod{m_1 m_2 \cdots m_k} \qquad (1)$$

等价于同余式組

$$f(x)\equiv 0 \pmod{m_1},\ f(x)\equiv 0 \pmod{m_2},\ \cdots,\ f(x)\equiv 0 \pmod{m_k}.$$

这时，設用 $T_1, T_2, \cdots, T_k$ 分别表示这个組里各个同余式的解的个数，而用 T 表示同余式(1)的解的个数，我們就有

$$T=T_1 T_2 \cdots T_k.$$

实际上，定理的第一部分可以从第三章 § 3, c 和 d 内推出。第二部分則从下面的事实得出：每个同余式

$$f(x)\equiv 0 \pmod{m_s}, \qquad (2)$$

在而且只在下列 T_s 个同余式有一个成立时才成立：

$$x\equiv b_s \pmod{m_s},$$

这里 b_s 通过同余式(2)的解答的剩余，并且总可以把全部 $T_1 T_2 \cdots$ $\cdots T_k$ 个不同的組合

$$x\equiv b_1 \pmod{m_1},\ x\equiv b_2 \pmod{m_2},\ \cdots,\ x\equiv b_k \pmod{m_k}$$

引向(按照 § 3, c)对于模 $m_1 m_2 \cdots m_k$ 的不同的类。

例子 同余式

$$f(x)\equiv 0 \pmod{35},\quad f(x)\equiv x^4+2x^3+8x+9 \qquad (3)$$

等价于同余式組

$$f(x)\equiv 0 \pmod 5,\ f(x)\equiv 0 \pmod 7.$$

从 § 1 很容易知道，这个組的第一个同余式有 2 个解答：$x\equiv$ $\equiv 1, 4 \pmod 5$，而第二个同余式有 3 个解答：$x\equiv 3, 5, 6 \pmod 7$。所以同余式(3)有 $2\cdot 3=6$ 个解答。为了求出这 6 个解答，需要解 6 个組：

$$x \equiv b_1 \pmod 5),\ x \equiv b_2 \pmod 7), \qquad (4)$$

这里 b_1 通过两个值 $b_1=1, 4$, b_2 通过三个值 $b_2=3, 5, 6$。但是由于

$$35=5\cdot 7=7\cdot 5,\ 7\cdot 3\equiv 1 \pmod 5),\ 5\cdot 3\equiv 1 \pmod 7),$$

适合組(4)的全体 x 的值，可以表示成(§ 3, 6)

$$x \equiv 21\, b_1 + 15\, b_2 \pmod{35}.$$

所以同余式(3)的解答是

$$x \equiv 31;\ 26;\ 6;\ 24;\ 19;\ 34 \pmod{35}.$$

b. 根据 a 的定理，研究和解同余式

$$f(x) \equiv 0 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}},$$

可以簡化成研究和解同余式

$$f(x) \equiv 0 \pmod{p^{\alpha}}; \qquad (5)$$

而这后一种同余式，我們現在就要来說明，它一般地可以簡化成同余式

$$f(x) \equiv 0 \pmod p. \qquad (6)$$

实际上，适合同余式(5)的每一个 x，一定也适合同余式(6)。設

$$x \equiv x_1 \pmod p$$

是同余式(6)的任意一个解。那末 $x=x_1+pt_1$，这里 t_1 是整数。把 x 的这个値代入同余式

$$f(x) \equiv 0 \pmod{p^2},$$

而且把左边按泰乐(Taylor)公式展开，我們求得(由于 $\frac{1}{k!}f^{(k)}(x_1)$ 是整数而且凡是 p^2 的倍数的各項都可以去掉)：

$$f(x_1)+pt_1f'(x_1) \equiv 0 \pmod{p^2},\ \frac{f(x_1)}{p}+t_1f'(x_1) \equiv 0 \pmod p.$$

在这里限于 $f'(x_1)$ 不被 p 除尽的情形，我們有一个解答：

$$t_1 \equiv t'_1 \pmod p;\ \ t_1 = t'_1 + pt_2.$$

把 x 表示成 $\qquad x = x_1 + pt'_1 + p^2 t_2 = x_2 + p^2 t_2;$

把它代入同余式 $f(x)\equiv 0 \pmod{p^3}$,

我們得到 $f(x_2)+p^2t_2f'(x_2)\equiv 0 \pmod{p^3}$,

$$\frac{f(x_2)}{p^2}+t_2f'(x_2)\equiv 0 \pmod{p}.$$

这里因为 $x_2\equiv x_1 \pmod{p}$,

$$f'(x_2)\equiv f'(x_1) \pmod{p},$$

$f'(x_2)$ 不被 p 除尽，所以最后得到的那个同余式有一个解答

$$t_2\equiv t'_2 \pmod{p};\ t_2=t'_2+pt_3.$$

把x表示成 $x=x_2+p^2t'_2+p^3t_3=x_3+p^3t_3$,

再繼續下去。利用同余式(6)的已知解答，我們可以用上述方法逐步地求出与它同余的同余式(5)的解答来。总之，同余式(6)的每一个解答 $x\equiv x_1 \pmod{p}$，在 $f'(x_1)$ 不被 p 除尽的条件下，給出同余式(5)的一个解答:

$$x=x_\alpha+p^\alpha t_\alpha;\ x\equiv x_\alpha \pmod{p^\alpha}.$$

例子 解同余式

$$f(x)\equiv 0 \pmod{27};\ f(x)=x^4+7x+4. \tag{7}$$

同余式 $f(x)\equiv 0 \pmod{3}$ 有一个解答 $x\equiv 1 \pmod{3}$; 由于 $f'(1)\equiv 2 \pmod{3}$, 因此它不被 3 除尽。我們得出

$$x=1+3t_1,$$

$$f(1)+3t_1f'(1)\equiv 0 \pmod{9},\ 3+3t_1\cdot 2\equiv 0 \pmod{9},$$

$$2t_1+1\equiv 0 \pmod{3},\ t_1\equiv 1 \pmod{3},\ t_1=1+3t_2,$$

$$x=4+9t_2.$$

$$f(4)+9t_2f'(4)\equiv 0 \pmod{27},\ 18+9t_2\cdot 2\equiv 0 \pmod{27},$$

$$2t_2+2\equiv 0 \pmod{3},\ t_2\equiv 2 \pmod{3},\ t_2=2+3t_3,$$

$$x=22+27t_3.$$

因此同余式(7)有一个解答:

$$x\equiv 22 \pmod{27}.$$

問　題

1, a. 設 m 是整数，$m>0$，$f(x,\cdots,w)$ 是 r 个变数 $x,\cdots,w$（$r\geqslant 1$）的有整系数的整有理函数。如果同余式

$$f(x,\cdots,w)\equiv 0 \pmod m \qquad (1)$$

有一組解答 $x=x_0,\cdots,w=w_0$，則（§1 的定义的推广）模 m 的数类的組：

$$x\equiv x_0 \pmod m,\ \cdots,\ w\equiv w_0 \pmod m$$

算做同余式(1)的一个解答。

設 T 是同余式(1)的解答的个数。証明

$$Tm=\sum_{a=0}^{m-1}\sum_{x=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{af(x,\cdots,w)}{m}}.$$

b. 在問題 a 和第三章問題 12, e 的表示式下，証明

$$Tm=m^r\sum_{m_0\diagdown m}A(m_0).$$

c. 应用問題 a 的等式来証明关于一次同余式的解答个数的定理。

d. 設 m 是整数，$m>0$；$a,\cdots,f,g$ 都是整数，它們的个数等于 $r+1$（$r>0$）；$d=(a,\cdots,f,m)$；T 是下列同余式的解答的个数：

$$ax+\cdots+fw+g\equiv 0 \pmod m.$$

利用問題 a 的等式，証明

$$T=\begin{cases} m^{r-1}d, & \text{如果 } g \text{ 是 } d \text{ 的倍数;}\\ 0, & \text{其他情形。}\end{cases}$$

e. 从关于同余式 $ax\equiv b \pmod m$ 的解答个数的定理出發，証明問題 a 的定理。

2, a. 設 $m>1$，$(a,m)=1$。証明同余式 $ax\equiv b \pmod m$ 有解

答

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

b. 設 p 是素数，$0<a<p$。証明同余式 $ax\equiv b \pmod{p}$ 有解答

$$x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{1\cdot 2\cdots a} \pmod{p}.$$

c, α) 指出解下列同余式的最簡單的方法:

$$2^k x \equiv b \pmod{m};\ (2, m)=1.$$

β) 指出解下列同余式的最簡單的方法:

$$3^k x \equiv b \pmod{m};\ (3, m)=1.$$

γ) 設 $(a, m)=1, 1<a<m$。推广問題 α) 和 β) 里的方法，証明，要求得同余式 $ax\equiv b \pmod{m}$ 的解答，可以化成求同余式 $b+mt\equiv 0 \pmod{p}$（p 是 a 的素約数）的解答。

3. 設 m 是整数，$m>1, 1\leqslant \tau<m, (a, m)=1$。利用同余式理論，証明有下列条件的整数 x 和 y 的存在:

$$ax\equiv y \pmod{m},\ 0<x\leqslant\tau,\ 0<|y|<\frac{m}{\tau}.$$

4, a. 当 $(a, m)=1$ 时，我們对于模 m 来討論符号分数 $\frac{b}{a}$，它表示同余式 $ax\equiv b \pmod{m}$ 的解的任意剩余。証明，（同余式都对模 m 而言）

α) 当 $a\equiv a_1, b\equiv b_1$ 时，我們有 $\frac{a}{b}\equiv\frac{a_1}{b_1}$。

β) 符号分数 $\frac{b}{a}$ 的分子 b 可以換成 a 的与 b 同余的倍数 b_0。于是符号分数就与由通常的分数 $\frac{b_0}{a}$ 表示的整数同余。

γ) $\frac{b}{a}+\frac{d}{c}\equiv\frac{bc+ad}{ac}$.

δ) $\frac{b}{a}\cdot\frac{d}{c}\equiv\frac{bd}{ac}$.

b, α) 設 p 是素数，$p>2$，a 是整数，$0<a<p-1$。証明

$$\binom{p-1}{a} \equiv (-1)^a \pmod p.$$

β) 設 p 是素数，$p>2$。証明

$$\frac{2^p-2}{p} \equiv 1-\frac{1}{2}+\frac{1}{3}-\cdots-\frac{1}{p-1} \pmod p.$$

5, a. 設 d 是 a 的約数，不被小于 n 的素数除尽。κ 是 d 的不同的素約数的个数，証明在数列

$$1\cdot 2\cdots n,\ 2\cdot 3\cdots(n+1),\ \cdots,\ a(a+1)\cdots(a+n-1) \qquad (1)$$

中，d 的倍数的个数是 $\frac{n^\kappa a}{d}$。

b. 設 $p_1, p_2, \cdots, p_k$ 是 a 的不同的素約数，沒有一个小于 n。証明在数列(1)中与 a 互素的数目的个数是

$$a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\cdots\left(1-\frac{n}{p_k}\right).$$

6. 設 $m_{1,2,\cdots,k}$ 是 $m_1, m_2, \cdots, m_k$ 的最小公倍数。

a. 設 $d=(m_1, m_2)$。証明同余式組

$$x\equiv b_1 \pmod{m_1},\ x\equiv b_2 \pmod{m_2}$$

在而且只在 b_2-b_1 是 d 的倍数时才能解，而且在可解时，所有适合这个組的 x 的值，由下面的同余式决定：

$$x\equiv x_{1,2} \pmod{m_{1,2}}.$$

b. 証明在同余式組

$$x\equiv b_1 \pmod{m_1},\ x\equiv b_2 \pmod{m_2},\ \cdots,\ x\equiv b_k \pmod{m_k}$$

可解的情形下，所有适合它們的 x 的值，由下面的同余式决定

$$x\equiv x_{1,2,\cdots,k} \pmod{m_{1,2,\cdots,k}}.$$

7. 設 m 是整数，$m>1$，a 和 b 都是整数，

$$\left(\frac{a,\ b}{m}\right)=\sum_x e^{2\pi i\frac{ax+bx'}{m}},$$

这里 x 通过与模 m 互素的剩余組，并且 $x'\equiv\frac{1}{x} \pmod m$(在問題 4,

a 的意义下)。証明符号 $\left(\frac{a,b}{m}\right)$ 的下列性質:

α) $\left(\frac{a,b}{m}\right)$ 是实数;

β) $\left(\frac{a,b}{m}\right)=\left(\frac{b,a}{m}\right)$;

γ) 当 $(h,m)=1$ 时，我們有 $\left(\frac{a,bh}{m}\right)=\left(\frac{ah,b}{m}\right)$;

δ) 設 $m_1, m_2, \cdots, m_k$ 兩兩互素，假設 $m_1 m_2 \cdots m_k = m$, $m = m_s M_s$, 我們有

$$\left(\frac{a_1,1}{m_1}\right)\left(\frac{a_2,1}{m_2}\right)\cdots\left(\frac{a_k,1}{m_k}\right)=\left(\frac{M_1^2 a_1+M_2^2 a_2+\cdots+M_k^2 a_k,1}{m}\right).$$

8. 設同余式

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n \equiv 0 \pmod p$$

有 n 个解: $x \equiv x_1, x_2, \cdots, x_n \pmod p$.

証明

$$a_1 \equiv -a_0 S_1 \pmod p,$$
$$a_2 \equiv \quad a_0 S_2 \pmod p,$$
$$a_3 \equiv -a_0 S_3 \pmod p,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_n \equiv (-1)^n a_0 S_n \pmod p,$$

这里 S_1 是所有 x_s 的总和，S_2 是每兩个 x_s 的乘积的总和，S_3 是每三个 x_s 的乘积的总和，等等。

9, a. 考虑数列 $2, 3, \cdots, p-2$ 中适合条件 $xx' \equiv 1 \pmod p$ 的每一对 x, x'，来証明威尔逊定理。

b. 設 P 是整数，$P>1$, $1\cdot2\cdots(P-1)+1\equiv 0 \pmod P$。証明 P 是素数。

10, a. 設 $(a_0, m)=1$，証明首項系数为 1 的 n 次同余式 $(n>0)$ 等价于同余式

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n \equiv 0 \pmod m.$$

b. 証明,同余式

$$f(x)\equiv 0 \pmod p;\ f(x)=x^n+a_1x^{n-1}+\cdots+a_n;\ n\leqslant p$$

有 n 个解答的必要而且充分的条件,是 x^p-x 被 $f(x)$ 除所得余式的所有系数都能被 p 除尽。

c. 設 n 是 $p-1$ 的約数,$n>1$;$(A,p)=1$。証明,同余式 $x^n\equiv\equiv A \pmod p$ 能解的必要而且充分的条件是 $A^{\frac{p-1}{n}}\equiv 1 \pmod p$,并且在可解的情形下,已知同余式有 n 个解答。

11. 設 n 是整数,$n>0$,$(A,m)=1$,而且已知同余式 $x^n\equiv A \pmod m$ 的一个解答 $x\equiv x_0 \pmod m$。証明这个同余式的所有解答可以用 x_0 乘上同余式 $y^n\equiv 1 \pmod m$ 的解答的剩余来表示。

計 算 題

1, a. 解同余式 $256x\equiv 179 \pmod{337}$。

b. 解同余式 $1215x\equiv 560 \pmod{2755}$。

2, a. 用問題 2, c 的方法解題 1, a 和 b 的同余式。

b. 用問題 2, c 的方法解同余式 $1296x\equiv 1105 \pmod{2413}$。

3. 求出适合不定方程 $47x-111y=89$ 的所有各对 x, y 来。

4, a. 指出下列同余式組的公共解答:

$$x\equiv b_1 \pmod{13},\ x\equiv b_2 \pmod{17}.$$

利用这个公共的解答,求被 13 和 17 除时分别給出对应的余数: 1 和 12, 6 和 8, 11 和 4 的三个数目。

b. 指出下列同余式組的公共解答:

$$x\equiv b_1 \pmod{25},\ x\equiv b_2 \pmod{27},\ x\equiv b_3 \pmod{59}.$$

5, a. 解同余式組:

$$x\equiv 3 \pmod 8,\ x\equiv 11 \pmod{20},\ x\equiv 1 \pmod{15}.$$

b. 解同余式組:

$$x\equiv1(\mathrm{mod}\ 3),\ x\equiv4(\mathrm{mod}\ 5),\ x\equiv2(\mathrm{mod}\ 7),$$
$$x\equiv9(\mathrm{mod}\ 11),\ x\equiv3(\mathrm{mod}\ 13).$$

6. 解同余式組:

$$3x+4y-29\equiv0(\mathrm{mod}\ 143),\ 2x-9y+84\equiv0(\mathrm{mod}\ 143).$$

7, a. 那一个次数低于 5 的同余式等价于同余式

$$3x^{14}+4x^{13}+3x^{12}+2x^{11}+x^9+2x^8+4x^7+x^6+3x^4+ \\ +x^3+4x^2+2x\equiv0(\mathrm{mod}\ 5)?$$

b. 那一个次数低于 7 的同余式等价于同余式

$$2x^{17}+6x^{16}+x^{14}+5x^{12}+3x^{11}+2x^{10}+x^9+5x^8+ \\ +2x^7+3x^5+4x^4+6x^3+4x^2+x+4\equiv0(\mathrm{mod}\ 7)?$$

8. 那一个首項系数为 1 的同余式等价于同余式(問題 10, a)

$$70x^6+78x^5+25x^4+68x^3+52x^2+4x+3\equiv0(\mathrm{mod}\ 101)?$$

9, a. 解同余式:

$$f(x)\equiv0(\mathrm{mod}\ 27),\ f(x)=7x^4+19x+25.$$

首先求出帮助用的下列同余式的所有解答:

$$f(x)\equiv0(\mathrm{mod}\ 3).$$

b. 解同余式 $9x^2+29x+62\equiv0(\mathrm{mod}\ 64)$。

10, a. 解同余式 $x^3+2x+2\equiv0(\mathrm{mod}\ 125)$。

b. 解同余式 $x^4+4x^3+2x^2+2x+12\equiv0(\mathrm{mod}\ 625)$。

11, a. 解同余式 $6x^3+27x^2+17x+20\equiv0(\mathrm{mod}\ 30)$。

b. 解同余式 $31x^4+57x^3+96x+191\equiv0(\mathrm{mod}\ 225)$。

第五章 二次同余式

§1. 一般性定理

a. 关于次数 $n>1$ 的同余式，在后面只討論比較簡單的二項同余式:

$$x^n \equiv a \pmod m), (a, m)=1. \tag{1}$$

如果同余式(1)有解，則 a 叫做 n 次剩余，否則 a 就叫做 n 次非剩余。特別地，当 $n=2$ 时，剩余或者非剩余都叫做平方的，当 $n=3$ 时則叫做立方的，当 $n=4$ 时，叫做双二次的。

b. 在这一章里我們要詳細討論 $n=2$ 的情形。現在先討論模是奇素数 p 的二次二項同余式:

$$x^2 \equiv a \pmod p), (a, p)=1. \tag{2}$$

c. 如果 a 是模 p（奇素数）的平方剩余，則同余式(2)有兩个解答。

实际上，如果 a 是平方剩余，則同余式 (2) 至少有一个解答 $x \equiv x_1 \pmod p$。于是由于 $(-x_1)^2=x_1^2$，这同一个同余式还有第二个解答 $x \equiv -x_1 \pmod p$。这第二个解答与第一个不同，因为从 $x_1 \equiv -x_1 \pmod p$ 我們將会有 $2x_1 \equiv 0 \pmod p$，由于 $(2, p)=(x_1, p)=1$，这是不可能的。

所指出的兩个解答已經穷尽了同余式 (2) 的全部解答，这是因为这同余式是二次的，它不可能有多于兩个的解答（第四章 §4, c)。

d. 与模 p 互素的剩余組，由 $\frac{p-1}{2}$ 个与数

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2 \tag{3}$$

同余的平方剩余，和$\frac{p-1}{2}$个平方非剩余組成。

实际上，在与模 p 互素的剩余組中出現的平方剩余，是而且只是与数（与模互素的剩余組）

$$-\frac{p-1}{2}, \cdots, -2, -1, 1, 2, \cdots, \frac{p-1}{2} \tag{4}$$

的平方，也就是(3)里的数，同余的那一些数。这时(3)里的数对于模 p 沒有同余的，因为从 $k^2 \equiv l^2 \pmod p$, $0<k<l\leqslant\frac{p-1}{2}$，推出，同余式 $x^2 \equiv l^2 \pmod p$ 在(4)的数中間有四个解答：$x=-l, -k, k, l$，与 c 矛盾。

e. 如果 a 是模 p 的平方剩余，則

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p; \tag{5}$$

而如果 a 是模 p 的平方非剩余，則

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p。 \tag{6}$$

实际上，从弗尔馬定理，

$$a^{p-1} \equiv 1 \pmod p; (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod p.$$

后一同余式左边的因子有一个而且只有一个能被 p 除尽（两个因子不能同时被 p 除尽，否則它們的差数 2 就要被 p 除尽了）。所以同余式(5)和(6)有一个而且只有一个成立。

但是每一个平方剩余 a，总会对于某个 x，适合同余式

$$a \equiv x^2 \pmod p, \tag{7}$$

把同余式(7)两边自乘 $\frac{p-1}{2}$ 次就得到同余式(5)，因此 a 也适合同余式(5)。这时因为同余式(5)是 $\frac{p-1}{2}$ 次的同余式，不能有多于

$\frac{p-1}{2}$ 个的解答，以致平方剩余就穷尽了它的全部解答

所以平方非剩余适合同余式(6)。

§2. 勒祥德兒符号

a. 讓我們在討論中引用勒祥德兒 (Legendre) 符号$\left(\frac{a}{p}\right)$ (讀做 a 对于 p 的勒祥德兒符号)。这个符号对于不被 p 除尽的所有 a 都有定义；当 a 是平方剩余时，它等于 1，当 a 是平方非剩余时，它等于 -1。数 a 和 p 分别叫做勒祥德兒符号的分子和分母。

b. 根据 §1, e, 明显地，我們有

$$\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}\ (\bmod p).$$

c. 現在我們来引出勒祥德兒符号的主要性質，在下一节里我們还將引出这个符号的推广——雅可比 (Jacobi) 符号的性質，这些性質使我們能迅速地計算这个符号，因而能迅速地解决下列同余式是否成立的問題：

$$x^2\equiv a\ (\bmod p).$$

d. 如果 $a\equiv a_1\ (\bmod p)$，則$\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$。

这个性質从下面的事实得来：屬于同一个类的数同时是平方剩余或者平方非剩余。

e. $\left(\frac{1}{p}\right)=1.$

实际上，$1=1^2$，因此 1 是平方剩余。

f. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$

这性質直接从 b 得出，只要讓 $a=-1$。

因为当 p 有形式 $4m+1$ 时，$\frac{p-1}{2}$是偶数，而当 p 有形式 $4m+$

$+3$ 时，$\frac{p-1}{2}$ 是奇数。所以对于形式 $4m+1$ 的素数，-1 是平方剩余，而对于形式 $4m+3$ 的素数，-1 是平方非剩余。

g. $\left(\frac{ab\ldots l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right)$.

实际上，我們有

$$\left(\frac{ab\ldots l}{p}\right)\equiv(ab\ldots l)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\ldots l^{\frac{p-1}{2}}\equiv$$

$$\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right)(\operatorname{mod} p),$$

于是就得出我們的断言。由此还推出

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right),$$

这就是說，在符号的分子里可以去掉任意的平方因子。

h. 为了引出勒祥德兒符号的进一步的性質，我們先給它以另外的解釋。假設 $p_1=\frac{p-1}{2}$，我們来討論同余式組

$$\left.\begin{array}{l} a\cdot 1\equiv\varepsilon_1 r_1 \;(\operatorname{mod} p), \\ a\cdot 2\equiv\varepsilon_2 r_2 \;(\operatorname{mod} p), \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a\cdot p_1\equiv\varepsilon_{p_1} r_{p_1} \;(\operatorname{mod} p), \end{array}\right\} \qquad (1)$$

这里 $\varepsilon_x r_x$ 是 ax 的絕对最小剩余，r_x 是它的絕对値，因而 $\varepsilon_x=\pm1$。

数目 $a\cdot1,\ -a\cdot1, a\cdot2,\ -a\cdot2, \cdots, a\cdot p_1,\ -a\cdot p_1$ 組成与模 p 互素的剩余組(第三章 §5, c)；它們的絕对的最小剩余是 $\varepsilon_1 r_1,\ -\varepsilon_1 r_1, \varepsilon_2 r_2,\ -\varepsilon_2 r_2, \cdots, \varepsilon_{p_1} r_{p_1},\ -\varepsilon_{p_1} r_{p_1}$。后一个数列中的正数，也就是 $r_1, r_2, \cdots, r_{p_1}$，应該与 $1, 2, \cdots, p_1$ 相合(第三章 § 4, b)。

現在把同余式組(1)兩边乘起来而且約掉

$$1\cdot2\cdots p_1=r_1 r_2\cdots r_{p_1},$$

我們得到 $a^{\frac{p-1}{2}}\equiv\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1}(\operatorname{mod} p)$。于是我們有(b)

$$\left(\frac{a}{p}\right)=\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1} \qquad (2)$$

i. 上述勒祥德兒符号的表示式还可以給予更完善的形式。我們有

$$\left[\frac{2ax}{p}\right]=\left[2\left[\frac{ax}{p}\right]+2\left\{\frac{ax}{p}\right\}\right]=2\left[\frac{ax}{p}\right]+\left[2\left\{\frac{ax}{p}\right\}\right],$$

它是偶数还是奇数，就看 ax 的非負的最小剩余小于还是大于 $\frac{1}{2}p$，也就是看 $\varepsilon_x=1$ 还是 -1。由此，很明显地有

$$\varepsilon_x=(-1)^{\left[\frac{2ax}{p}\right]},$$

所以从(2)式我們得出

$$\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}.$$

j. 假設 a 是奇数，我們来作下列等式的变形。我們有（$a+p$ 是偶数）

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\frac{a+p}{2}}{p}\right)=\left(\frac{\frac{a+p}{2}}{p}\right)=$$

$$=(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]}=(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum\limits_{x=1}^{p_1}x},$$

于是

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}. \qquad (3)$$

公式(3)使我們得到勒祥德兒符号的兩个極重要的性質。

k. $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

在公式(3)里讓 $a=1$ 就得到它。

再有,因为

$$\frac{(8m\pm1)^2-1}{8}=8m^2\pm2m \quad 是偶数,$$

$$\frac{(8m\pm3)^2-1}{8}=8m^2\pm6m+1 \quad 是奇数,$$

所以由此推出，2 对于 $8m\pm1(8m+1,8m+7)$ 形式的素数是平方剩余,而对于 $8m\pm3(8m+3,8m+5)$形式的素数是平方非剩余。

1. 如果 p 和 q 都是奇素数,则(平方剩余的反逆法则)

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

因为 $\frac{p-1}{2}\cdot\frac{q-1}{2}$ 只有在 p 和 q 都有形式 $4m+3$ 时才是奇数,而且只要其中有一个有形式 $4m+1$,它就是偶数,所以所說的性質可以写成:

如果 p 和 q 都有形式 $4m+3$, 则

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right);$$

而如果其中有一个有形式 $4m+1$,则

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

为了証明,我們注意到,公式(3)根据 k 有形式:

$$\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{x=1}^{p_1}\left[\frac{ax}{p}\right]}. \tag{4}$$

現在假設 $\frac{q-1}{2}=q_1$, 来討論 p_1q_1 个数偶: qx, py, 这里 x 和 y 独立地通过

$$x=1,2,\cdots,p_1,\quad y=1,2,\cdots,q_1.$$

我們决不能有 $qx=py$，因为从这个等式將会得出 py 是 q 的倍数，根据$(p,q)=(y,q)=1$(因为 $0<y<q$) 这是不可能的。所以我們可以讓 $p_1q_1=S_1+S_2$，这里 S_1 是有 $qx<py$ 的数偶的个数，而 S_2 是有 $py<qx$ 的数偶的个数。

很明显地，S_1 还是适合 $x<\frac{p}{q}y$ 的数偶的个数。这里在給了 y 以后，可以取 $x=1,2,\cdots\left[\frac{p}{q}y\right]$。(根据$\frac{p}{q}y\leqslant\frac{p}{q}q_1<\frac{p}{2}$，我們有 $\left[\frac{p}{q}y\right]\leqslant p_1$)。因此

$$S_1=\sum_{y=1}^{q_1}\left[\frac{p}{q}y\right].$$

用同样的方法可以肯定

$$S_2=\sum_{x=1}^{p_1}\left[\frac{q}{p}x\right].$$

于是等式(4)給我們

$$\left(\frac{p}{q}\right)=(-1)^{S_1},\quad\left(\frac{q}{p}\right)=(-1)^{S_2},$$

所以
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{S_1+S_2}=(-1)^{p_1q_1}.$$

从这里就得出上述的性質。

§3. 雅可比符号

a. 为了更迅速地計算勒祥德兒符号，我們来討論更普遍的雅可比符号。設 P 是奇数，大于一，而且 $P=p_1p_2\cdots p_r$ 是它的素因子分解式（这些因子中間可以有相等的)。再設 $(a,P)=1$。那末雅可比符号$\left(\frac{a}{P}\right)$由下列等式定出：

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$$

勒祥德兒符号的已知性質，使我們能确立雅可比符号的类似性質。

b. 如果 $a\equiv a_1 \pmod{P}$，則 $\left(\frac{a}{P}\right)=\left(\frac{a_1}{P}\right)$。

实际上，因为对于模 P, a 与 a_1 同余，所以对于 P 的約数 p_1, $p_2, \cdots, p_r$, a 与 a_1 也同余，我們就有

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_r}\right)=\left(\frac{a_1}{P}\right).$$

c. $\left(\frac{1}{P}\right)=1.$

实际上，

$$\left(\frac{1}{P}\right)=\left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_r}\right)=1.$$

d. $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}.$

为了肯定这一点，我們注意到

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_r}\right)=$$

$$=(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_r-1}{2}}; \qquad (1)$$

但是

$$\frac{P-1}{2}=\frac{p_1p_2\cdots p_r-1}{2}=$$

$$=\frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\cdots\left(1+2\frac{p_r-1}{2}\right)-1}{2}=$$

$$=\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_r-1}{2}+2N.$$

根据这个，我們从公式(1)我們得出

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}.$$

e. $\left(\frac{ab\cdots l}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\cdots\left(\frac{l}{P}\right).$

实际上，

$$\left(\frac{ab\cdots l}{P}\right)=\left(\frac{ab\cdots l}{p_1}\right)\cdots\left(\frac{ab\cdots l}{p_r}\right)=$$

$$=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{l}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\cdots\left(\frac{l}{p_r}\right);$$

把有相同分子的符号聚集在一起，我們就得到所断定的性質。由此还推出

$$\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right).$$

f. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$

实际上，

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right)=$$

$$=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_r^2-1}{8}}. \qquad (2)$$

但是

$$\frac{P^2-1}{8}=\frac{p_1^2p_2^2\cdots p_r^2-1}{8}=$$

$$=\frac{\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right)\cdots\left(1+8\frac{p_r^2-1}{8}\right)-1}{8}=$$

$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_r^2-1}{8}+2N,$$

根据这个，我們从公式(2)得出

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

g. 如果 P 和 Q 是正的互素的奇数，则

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

实际上，設 $Q=q_1q_2\cdots q_s$ 是 Q 的素因子分解式（它們中間可以有相等的）。我們有

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\cdots\left(\frac{Q}{p_r}\right)=\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right)=$$

$$=(-1)^{\sum\limits_{\alpha=1}^{r}\sum\limits_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{q_\beta-1}{2}}\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right)=$$

$$=(-1)^{\left(\sum\limits_{\alpha=1}^{r}\frac{p_\alpha-1}{2}\right)\left(\sum\limits_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)}\left(\frac{P}{Q}\right).$$

但是，与在 d 里一样，我們有

$$\frac{P-1}{2}=\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}+2N,\quad \frac{Q-1}{2}=\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}+2N_1,$$

根据这个，上面的最后一个公式給出

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

例子 作为計算勒祥德兒符号（这时把它看作雅可比符号的特别情形）的例子，我們来研究下面的同余式是否有解答：

$$x^2\equiv 219 \pmod{383}.$$

我們有（依次应用 g, b 以及 e, g, b, e, f, g, b, d）

$$\left(\frac{219}{383}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{41}{219}\right)=$$
$$=-\left(\frac{219}{41}\right)=-\left(\frac{14}{41}\right)=-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)=$$
$$=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=1.$$

因此，已知的同余式有两个解答。

§4. 复合数模的情形

a. 复合数模的二次同余式，就按照第四章§5的一般性的討論来研究和解决。

b. 我們从下面形式的同余式开始:

$$x^2\equiv a \pmod{p^\alpha};\ \alpha>0,\ (a, p)=1, \tag{1}$$

这里 p 是奇素数。

假設 $f(x)=x^2-a$, 我們有 $f'(x)=2x$, 而如果 $x\equiv x_1 \pmod p$ 是同余式

$$x^2\equiv a \pmod p \tag{2}$$

的解答，則根据 $(a, p)=1$, 也有 $(x_1, p)=1$, 而因为 p 是奇数，所以 $(2x_1, p)=1$, 也就是說 $f'(x_1)$ 不被 p 除尽。所以要找出同余式(1)的解答，可以应用第四章§5, b 的論証，并且同余式(2)的每一个解答都給出同余式(1)的一个解答。上面的討論引出:

同余式(1)有两个解答或者一个也沒有，就看 a 对于模 p 是平方剩余还是平方非剩余。

c. 現在我們来討論同余式

$$x^2\equiv a \pmod{2^\alpha};\ \alpha>0,\ (a, 2)=1. \tag{3}$$

这里 $f'(x_1)=2x_1$ 被 2 除尽，因而不能应用第四章§5, b 的論証；它們应該被換成下面的方式:

d. 如果同余式(3)能解，則由于 $(a, 2)=1$，我們有 $(x, 2)=1$,

即 $x=1+2t$，这里 t 是整数。同余式(3)有形状

$$1+4t(t+1)\equiv a \pmod{2^\alpha}.$$

但是数 t 和 $t+1$ 中有一个是偶数，所以 $4t(t+1)$ 是 8 的倍数。因此，要使最后这个同余式能解，除同余式(3)外还必须有

$$a\equiv 1 \pmod 4 \text{ 对于 } \alpha=2;\ a\equiv 1 \pmod 8 \text{ 对于 } \alpha\geqslant 3. \quad (4)$$

e. 在不違反条件(4)的情形下，我們来討論求解答以及它們的个数的問題。

在 $\alpha\leqslant 3$ 的情形，根据 d，同余式被所有奇数所适合。所以同余式 $x^2\equiv a \pmod 2$ 有一个解答：$x\equiv 1 \pmod 2$，同余式 $x^2\equiv a \pmod 4$ 有两个解答：$x\equiv 1,\ 3 \pmod 4$，同余式 $x^2\equiv a \pmod 8$ 有四个解答：$x\equiv 1, 3, 5, 7 \pmod 8$。

为了討論 $\alpha=4, 5, \cdots$ 的情形，先把所有奇数分成兩个算术級数：

$$x=\pm(1+4t_3) \quad (5)$$

$$(1+4t_3\equiv 1 \pmod 4;\ -1-4t_3\equiv -1\equiv 3 \pmod 4).$$

我們察看 (5) 里有那一些数适合同余式 $x^2\equiv a \pmod{16}$。我們求得

$$(1+4t_3)^2\equiv a \pmod{16},\quad t_3\equiv\frac{a-1}{8} \pmod 2,$$

$$t_3=t_3'+2t_4,\quad x=\pm(1+4t_3'+8t_4)=\pm(x_4+8t_4).$$

我們再察看上面这些数中有那一些适合同余式 $x^2\equiv a \pmod{32}$。我們求得

$$(x_4+8t_4)^2\equiv a \pmod{32}, t_4=t_4'+2t_5, x=\pm(x_5+16t_5),$$

等等。用这样的方法可以肯定，对于任意的 $\alpha>3$，适合同余式(3)的 x 值，可以表示成

$$x=\pm(x_\alpha+2^{\alpha-1}t_\alpha).$$

x 的这些值組成同余式(3)的四个不同的解答：

$$x\equiv x_\alpha;\ x_\alpha+2^{\alpha-1};\ -x_\alpha;\ -x_\alpha-2^{\alpha-1} \pmod{2^\alpha}.$$

(对于模 4 前兩个与 1 同余,而后兩个則与 -1 同余。)

例子 同余式

$$x^2\equiv 57 \pmod{64}, \qquad (6)$$

根据 $57\equiv 1 \pmod 8$, 有四个解答。把 x 表成 $x=\pm(1+4t_3)$, 我們得出

$$(1+4t_3)^2\equiv 57 \pmod{16},\quad 8t_3\equiv 56 \pmod{16},$$
$$t_3\equiv 1 \pmod 2,\quad t_3=1+2t_4,\quad x=\pm(5+8t_4),$$
$$(5+8t_4)^2\equiv 57 \pmod{32},\quad 5\cdot 16t_4\equiv 32 \pmod{32},$$
$$t_4\equiv 0 \pmod 2,\quad t_4=2t_5,\quad x=\pm(5+16t_5),$$
$$(5+16t_5)^2\equiv 57 \pmod{64},\quad 5\cdot 32t_5\equiv 32 \pmod{64},$$
$$t_5\equiv 1 \pmod 2,\quad t_5=1+2t_6,\quad x=\pm(21+32t_6).$$

所以同余式(6)的解答是

$$x\equiv \pm 21, \pm 53 \pmod{64}.$$

f. 从 c, d 和 e 推出:

同余式

$$x^2\equiv a \pmod{2^\alpha},\ (2, a)=1$$

能解的必要条件是: $a\equiv 1 \pmod 4$ 当 $\alpha=2$; $a\equiv 1 \pmod 8$ 当 $\alpha\geqslant 3$。如果这个条件沒有違反,解答的个数是: 1, 当 $\alpha=1$; 2, 当 $\alpha=2$; 4, 当 $\alpha\geqslant 3$。

g. 从 b, f 和第四章 § 5, a 推出:

普遍形式的同余式

$$x^2\equiv a \pmod m;\ m=2^\alpha p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_k^{\alpha_k};\ (a, m)=1$$

能解的必要条件是:

$$a\equiv 1 \pmod 4 \text{ 当 } \alpha=2;\quad a\equiv 1 \pmod 8 \text{ 当 } \alpha\geqslant 3,$$

$$\left(\frac{a}{p_1}\right)=1, \left(\frac{a}{p_2}\right)=1, \cdots, \left(\frac{a}{p_k}\right)=1.$$

如果这些条件沒有一个違反, 解答的个数是: 2^k, 当 $\alpha=0$ 和 $\alpha=1$;

2^{k+1}，当 $\alpha=2$；2^{k+2}，当 $\alpha\geqslant 3$。

問　題

以下 p 总是表示奇素数。

1. 証明，要得出形式

$$ax^2+bx+c\equiv 0 \pmod{m},\ (2a, m)=1$$

的同余式的解答，可以从找出形式 $x^2\equiv q \pmod{m}$ 的同余式的解答着手。

2, a. 利用 §1, e, 找出下列同余式的解答(在可能的情形下)：

$$x^2\equiv a \pmod{p};\quad p=4m+3.$$

b. 利用 §2, b 和 k, 指出求下列同余式的解答的方法：

$$x^2\equiv a \pmod{p};\quad p=8m+5.$$

c. 在已知模 p 的一个平方非剩余 N 的情形下，指出求下列同余式解答的可能的比較簡單的方法：

$$x^2\equiv a \pmod{p};\quad p=8m+1.$$

d. 利用威尔逊定理，証明同余式

$$x^2+1\equiv 0 \pmod{p};\quad p=4m+1$$

的解答是

$$x\equiv \pm 1\cdot 2\cdots 2m \pmod{p}.$$

3, a. 証明，同余式

$$x^2+1\equiv 0 \pmod{p} \qquad (1)$$

能解，如果而且只如果 p 有形式 $4m+1$；同余式

$$x^2+2\equiv 0 \pmod{p} \qquad (2)$$

能解，如果而且只如果 p 有形式 $8m+1$ 或者 $8m+3$；同余式

$$x^2+3\equiv 0 \pmod{p} \qquad (3)$$

能解，如果而且只如果 p 有形式 $6m+1$。

b. 証明 $4m+1$ 形式的素数的个数是無限的。

c. 証明 $6m+1$ 形式的素数的个数是無限的。

4. 設数目 $1, 2, \cdots, p-1$ 分成兩个集合，其中第二个集合包含着不少于一个的数，我們有：同一集合的兩个数的乘积对于模 p 与第一个集合里的一个数同余，而不同集合的兩个数的乘积对于模 p 与第二个集合里的一个数同余。証明，这种情形成立的必要而且充分的条件是：第一个集合由模 p 的平方剩余組成，而第二个集合則由平方非剩余組成。

5, a. 把 a 和 x 表示成 p 进位的数，引出关于下列同余式的理論：

$$x^2 \equiv a \pmod{p^\alpha};\quad (a, p)=1.$$

b. 把 a 和 x 表示成 2 进位的数，引出关于下列同余式的理論：

$$x^2 \equiv a \pmod{2^\alpha};\quad (a, 2)=1.$$

6. 証明同余式

$$x^2 \equiv a \pmod{p^\alpha},\ (a, p)=1$$

的解答是 $x \equiv \pm PQ' \pmod{p^\alpha}$，这里

$$P=\frac{(z+\sqrt{a})^\alpha+(z-\sqrt{a})^\alpha}{2},\quad Q=\frac{(z+\sqrt{a})^\alpha-(z-\sqrt{a})^\alpha}{2\sqrt{a}},$$

$$z^2 \equiv a \pmod{p},\quad QQ' \equiv 1 \pmod{p^\alpha}.$$

7. 从同余式 $x^2 \equiv 1 \pmod{m}$ 与同余式 $(x-1)(x+1) \equiv 0 \pmod{m}$ 等价的事实，指出解这个同余式的方法。

8. 設 $\left(\frac{a}{p}\right)=0$ 对于 $(a, p)=p$。

a. 当 $(k, p)=1$ 时，証明

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=-1.$$

b. 設 ε 和 η 都等于 $+1$ 或者 -1，T 是有条件 $\left(\frac{x}{p}\right)=\varepsilon$，$\left(\frac{x+1}{p}\right)=\eta$ 的数偶 $x, x+1$（这里 $x=1, 2, \cdots, p-2$）的个数。証明

$$T=\frac{1}{4}\left(p-2-\varepsilon\left(\frac{-1}{p}\right)-\eta-\varepsilon\eta\right).$$

c. 設 $(k, p)=1$，

$$S=\sum_x\sum_y\left(\frac{xy+k}{p}\right),$$

这里 x 和 y 对应地通过由 X 和 Y 个模 p 的完全剩余組的剩余組成的遞增数列。証明

$$|S|<\sqrt{2XYp}.$$

为了証明，应該利用不等式

$$|S|^2\leqslant X\sum_x\left|\sum_y\left(\frac{xy+k}{p}\right)\right|^2.$$

d. 設 Q 是整数，$1<Q<p$，

$$S=\sum_{x=0}^{p-1}S_x^2;\quad S_x=\sum_{z=0}^{Q-1}\left(\frac{x+z}{p}\right).$$

α）証明 $S=(p-Q)Q$。

β）設 λ 是常数，$0<\lambda<1$。証明，数列 $x=0, 1, \cdots, p-1$ 中不合于条件 $S_x\leqslant Q^{0.5+0.5\lambda}$ 的数的个数 T，适合条件 $T\leqslant pQ^{-\lambda}$。

γ）設 $p>25$，M 是整数。証明在数列

$$M, M+1, \cdots, M+3[\sqrt{p}]-1$$

中有着模 p 的平方非剩余。

9, a. 証明，整数 $m>1$ 中能表成

$$m=x^2+y^2,\ (x, y)=1,\ x>0,\ y>0 \tag{1}$$

的个数，等于下列同余式的解答的个数：

$$z^2+1\equiv 0 \pmod{m}. \tag{2}$$

为了証明，讓 $\tau=\sqrt{m}$，按照第一章問題4, b的定理，利用 $\alpha=\frac{z}{m}$ 的表示式，再討論用 Q^2 乘(2)式得到的同余式。

b. 設 a 是2和3的一个。証明，有条件 $p>a$ 的素数 p 中可以表示成

$$p=x^2+ay^2,\quad x>0, y>0 \tag{3}$$

的个数，等于下列同余式的解答的个数：

$$z^2+a\equiv 0 \pmod{p}. \tag{4}$$

c. 設 p 有形式 $4m+1$, $(k, p)=1$,

$$S(k)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right).$$

証明(高尔士可夫[Д. С. Горшков])

α) $S(k)$ 是偶数。

β) $S(kt^2)=\left(\frac{t}{p}\right)S(k)$.

γ) 当 $\left(\frac{r}{p}\right)=1$, $\left(\frac{n}{p}\right)=-1$, 我們有(参看問題a)

$$p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2.$$

10. 設 D 是正整数，不是平方数。証明：

a. 如果对于已知整数 k，方程

$$x^2-Dy^2=k$$

有两对解答 $x=x_1, y=y_1$ 和 $x=x_2, y=y_2$，則方程

$$X^2-DY^2=k^2$$

被下列等式中的 X 和 Y 所适合(±号任意选擇)：

$$X+Y\sqrt{D}=(x_1+y_1\sqrt{D})(x_2\pm y_2\sqrt{D}).$$

b. 方程(沛尔[Pell]方程)

$$x^2-Dy^2=1 \qquad (1)$$

有正整数 x, y 的解答。

c. 如果 x_0, y_0 是适合(1)式的正数偶 x, y 中有最小 x（或者是等价条件，有最小 $x+y\sqrt{D}$）的，则所有适合这方程的正数偶 x, y 可以由下面的等式来表示：

$$x+y\sqrt{D}=(x_0+y_0\sqrt{D})^r; \quad r=1, 2, \cdots. \qquad (2)$$

11, a. 設 a 是整数，

$$U_{a,p}=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{ax}{p}}.$$

α) 当 $(a, p)=1$，証明 $|U_{a,p}|=\sqrt{p}$。

为了証明，和式 $U_{a,p}$ 应該乘上把 i 换成 $-i$ 而得到的共軛数。用 x 和 x_1 分别表示 $U_{a,p}$ 和它的共軛数对之求和的变数，应該聚集这样的乘积項，在那里对于已知的 t 有

$$x_1\equiv xt \pmod p$$

或者
$$x_1\equiv x+t \pmod p.$$

β) 証明

$$\left(\frac{a}{p}\right)=\frac{U_{a,p}}{U_{1,p}}.$$

b. 設 $m>2, (a, m)=1$,

$$S_{a,m}=\sum_{x=0}^{m-1}e^{2\pi i\frac{ax^2}{m}}.$$

α) 証明 $S_{a,p}=U_{a,p}$。（問題 a）

β) 从問題 α) 和問題 a, α) 的定理推出 $|S_{a,p}|=\sqrt{p}$。証明下列更普遍的結果：

$$|S_{a,m}|=\sqrt{m}, \quad 如果\ m\equiv 1 \pmod 2,$$

$$|S_{a,m}|=0,\qquad 如果\ m\equiv 2\pmod 4,$$

$$|S_{a,m}|=\sqrt{2m},\ 如果\ m\equiv 0\pmod 4)。$$

γ) 設 $m>1$, $(2A, m)=1$, a 是任意整数。証明

$$\left|\sum_{x=0}^{m-1} e^{2\pi i\frac{Ax^2+ax}{m}}\right|=\sqrt{m}.$$

12, a. 設 m 是大于 1 的整数，M 和 Q 都是整数，$0\leqslant M<M+$ $+Q\leqslant m$, $\sum\limits_{z}$ 表示在給定的整数集合上对 z 展开的和式，而 $\sum\limits_{z}{}'$ 則表示只对这集合中对于模 m 与

$$M, M+1, \cdots, M+Q-1$$

同余的数 z 展开的和式。再設函数 $\Phi(x)$ 是这样的：对于某个 Δ 和任意的 $a=1, 2, \cdots, m-1$, 都有

$$\left|\sum_{z}\Phi(z)e^{2\pi i\frac{az}{m}}\right|\leqslant\Delta.$$

証明
$$\sum_{z}{}'\Phi(z)=\frac{Q}{m}\sum_{z}\Phi(z)+\theta\Delta(\ln m-\delta),$$

这里 $|\theta|<1$, $\delta>0$, 并且当 $m\geqslant 12$ 时 $\delta>\frac{1}{2}$; 当 $m\geqslant 60$ 时 $\delta>1$。

b. 設 M 和 Q 都是整数，$0<M<M+Q\leqslant p$。

α) 証明

$$\left|\sum_{x=M}^{M+Q-1}\left(\frac{x}{p}\right)\right|<\sqrt{p}\ln p.$$

β) 設 R 和 N 分別是在数列 $M, M+1, \cdots, M+Q-1$ 中的平方剩余和平方非剩余的个数。証明

$$R=\frac{1}{2}Q+\frac{\theta}{2}\sqrt{p}\ln p,\ N=\frac{1}{2}Q-\frac{\theta}{2}\sqrt{p}\ln p;\ |\theta|<1.$$

γ) 利用問題 a 和問題 11, b, β) 里的定理，引出問題 β) 的公式。

δ) 設 $m\geqslant 60$, $(2A, m)=1$, M_0 和 Q_0 都是整数，$0<M_0<M_0+Q_0\leqslant m$。証明

$$\left|\sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i\frac{Ax^2}{m}}\right|<\sqrt{m}\ln m.$$

ε) 設 $p>60$, $(A, p)=1$, M_0 和 Q_0 都是整数，$0<M_0<M_0+Q_0\leqslant p$, 而且 T 表示数列 Ax^2, $x=M_0, M_0+1, \cdots, M_0+Q_0-1$ 中对于模 p 与数列 $M, M+1, \cdots, M+Q-1$ 的数同余的数的个数。証明

$$T=\frac{Q_0Q}{p}+\theta\sqrt{p}(\ln p)^2.$$

c. 討論下列和式，引出問題 b, β) 的公式:

$$\sum_{a=0}^{p-1}\sum_{\alpha=1}^{p-1}\sum_{x=M}^{M+Q-1}\sum_{y=M}^{M+Q-1}\left(\frac{\alpha}{p}\right)e^{2\pi i\frac{a(x-\alpha y)}{p}}.$$

計 算 題

1, a. 在与模 23 互素的剩余組中指出平方剩余。

b. 在与模 37 互素的剩余組中指出平方非剩余。

2, a. 应用 § 1, e, 指出下列同余式的解答的个数:

α) $x^2\equiv 3 \pmod{31}$;

β) $x^2\equiv 2 \pmod{31}$.

b. 指出下列同余式的解答的个数:

α) $x^2\equiv 5 \pmod{73}$;

β) $x^2\equiv 3 \pmod{73}$.

3, a. 計算雅可比符号，指出下列同余式的解答的个数:

α) $x^2 \equiv 226 \pmod{563}$;

β) $x^2 \equiv 429 \pmod{563}$.

b. 指出下列同余式的解答的个数:

α) $x^2 \equiv 3766 \pmod{5987}$;

β) $x^2 \equiv 3149 \pmod{5987}$.

4, a. 应用問題 2, a; 2, b; 2, c 的方法,解同余式:

α) $x^2 \equiv 5 \pmod{19}$;

β) $x^2 \equiv 5 \pmod{29}$;

γ) $x^2 \equiv 2 \pmod{97}$.

b. 解同余式:

α) $x^2 \equiv 2 \pmod{311}$;

β) $x^2 \equiv 3 \pmod{277}$;

γ) $x^2 \equiv 11 \pmod{353}$.

5, a. 解同余式 $x^2 \equiv 59 \pmod{125}$,利用下列方法:

α) § 4, b; β) 問題 5, a; γ) 問題 6。

b. 解同余式 $x^2 \equiv 91 \pmod{243}$。

6, a. 解同余式 $x^2 \equiv 41 \pmod{64}$,利用下列方法:

α) § 4, e; β) 問題 5, b。

b. 解同余式 $x^2 \equiv 145 \pmod{256}$。

第六章　元根和指数

§1. 一般性定理

a. 对于$(a, m)=1$有着正的γ适合条件$a^{\gamma}\equiv 1 \pmod m$，例如$\gamma=\varphi(m)$（欧拉定理）这些数目中間最小的一个叫做$a$对于模$m$所屬的方次数。

b. 如果a对于模m屬于方次数δ，则$1=a^0, a^1, \cdots, a^{\delta-1}$对于模$m$都不同余。

实际上，从$a^l\equiv a^k \pmod m$ $0\leqslant k<l<\delta$，推出$a^{l-k}\equiv 1 \pmod m$，$0<l-k<\delta$，与δ的定义矛盾。

c. 如果a对于模m屬于方次数δ，则$a^{\gamma}\equiv a^{\gamma'} \pmod m$在而且只在$\gamma\equiv\gamma' \pmod \delta$时；特别地（当$\gamma'=0$），$a^{\gamma}\equiv 1 \pmod m$在而且只在$\gamma$被$\delta$除尽时。

实际上，設r和r_1是γ和γ'对于模δ的非負的最小剩余；那末就有着某两个q和q_1使得$\gamma=\delta q+r$，$\gamma'=\delta q_1+r_1$。由此再从$a^{\delta}\equiv 1 \pmod m$推出

$$a^{\gamma}\equiv (a^{\delta})^q a^r\equiv a^r \pmod m,$$

$$a^{\gamma'}\equiv (a^{\delta})^{q_1} a^{r_1}\equiv a^{r_1} \pmod m.$$

所以$a^{\gamma}\equiv a^{\gamma'} \pmod m$，在而且只在$a^r\equiv a^{r_1} \pmod m$也就是$r=r_1$时（**b**）。

d. 从$a^{\varphi(m)}\equiv 1 \pmod m$和从**c**（$\gamma'=0$）推出$\varphi(m)$被$\delta$除尽。所以任意数对于模$m$所屬的方次数都是$\varphi(m)$的約数。这些約数中最大的是$\varphi(m)$本身。屬于方次数$\varphi(m)$的数（如果存在的話）叫

做模 m 的元根。

§ 2. 模 p^α 和 $2p^\alpha$ 的元根

a. 設 p 是奇素数而且 $\alpha \geqslant 1$。我們来証明模 p^α 和 $2p^\alpha$ 的元根的存在。

b. 如果 x 对于模 m 屬于方次数 ab, 則 x^a 屬于方次数 b。

实际上，設 x^a 屬于方次数 δ。那末 $(x^a)^\delta \equiv 1 \pmod m$, 于是 $x^{a\delta} \equiv 1 \pmod m$; 因此 $a\delta$ 被 ab 除尽(§ 1, c), 卽 δ 被 b 除尽。另一方面，$x^{ab} \equiv 1 \pmod m$, 于是 $(x^a)^b \equiv 1 \pmod m$; 因此 b 被 δ 除尽(§ 1,c)。所以 $\delta = b$。

c. 如果 x 对于模 m 屬于方次数 a, 而 y 屬于方次数 b, 并且 $(a, b) = 1$, 則 xy 屬于方次数 ab。

实际上，設 xy 屬于方次数 δ。那末 $(xy)^\delta \equiv 1 \pmod m$。由此 $x^{b\delta} y^{b\delta} \equiv 1 \pmod m$, 而且 $x^{b\delta} \equiv 1 \pmod m$(§ 1, c)。所以 $b\delta$ 被 a 除尽(§ 1, c), 而且由于 $(b, a) = 1$, δ 被 a 除尽。同样地我們得出 δ 被 b 除尽。再由于 $(b, a) = 1$, δ 被 a 又被 b 除尽，也就被 ab 除尽。另一方面，从 $(xy)^{ab} \equiv 1 \pmod m$ 推出 ab 被 δ 除尽(§ 1, c)。所以 $\delta = ab$。

d. 对于模 p 有元根存在。

实际上，設

$$\delta_1, \delta_2, \cdots, \delta_\tau \tag{1}$$

是数 $1, 2, \cdots, p-1$ 中至少有一个对于模 p 所屬的方次数，而 τ 是这些方次数的最小公倍数，再設 $\tau = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ 是 τ 的标准分解式；那末对于每个 s, 在(1)的数中間总有着能被 $q_s^{\alpha_s}$ 除尽的某个 δ, 因而它可以表示成 $\delta = aq_s^{\alpha_s}$。如果 x 是屬于方次数 δ 的数，

則根据 b, $x_s=x^a$ 就屬于方次数 $q_s^{\alpha_s}$。对于 $s=1,2,\cdots,k$ 进行了这种討論以后；按照 c, 数 $g=x_1x_2\cdots x_k$ 屬于方次数 $q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_k^{\alpha_k}=\tau$。

但是由于(1)里的方次数全是数 τ 的約数，所以数 $1,2,\cdots,p-1$ 全都适合同余式 $x^\tau\equiv1\pmod p$(§ 1, c)。这說明 $p-1\leqslant\tau$(第四章 § 4, c)。但是 τ 又是 $p-1$ 的約数。所以 $\tau=p-1$, 这就是說，g 是元根。

e. 設 g 是模 p 的元根。可以找出适合下列条件的 t: 由等式 $(g+pt)^{p-1}=1+pu$ 决定的 u 不被 p 除尽。对于任意的 $\alpha>1$, 对应的 $g+pt$ 是模 p^α 的元根。

实际上，我們有

$$g^{p-1}=1+pT_0,$$

$$(g+pt)^{p-1}=1+p(T_0-g^{p-2}t+pT')=1+pu, \qquad (2)$$

这里 u 与 t 同时通过模 p 的完全剩余組。所以可以找出 t, 适合条件 u 不被 p 除尽。对于找到的 t, 从(2)式还得出

$$\left.\begin{aligned}&(g+pt)^{p(p-1)}=(1+pu)^p=1+p^2u_2,\\&(g+pt)^{p2(p-1)}=(1+p^2u_2)^p=1+p^3u_3,\\&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\end{aligned}\right\} \qquad (3)$$

这里 $u_2, u_3, \cdots$ 不被 p 除尽。

設 $g+pt$ 对于 p^α 屬于方次数 δ。那末

$$(g+pt)^\delta\equiv1\pmod{p^\alpha}. \qquad (4)$$

由此 $(g+pt)^\delta\equiv1\pmod p$, 因此 δ 是 $p-1$ 的倍数。又因为 δ 除尽 $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$, 所以 $\delta=p^r(p-1)$, 这里 r 是数 $1,2,\cdots,\alpha$ 中的一个。同余式(4)左边用等式(2)和(3)里它的对应的表示式来代替($u=u_1$), 我們得到

$$1+p^ru_r\equiv1\pmod{p^\alpha},\ p^r\equiv0\pmod{p^\alpha},\ r=\alpha,\ \delta=\varphi(p^\alpha),$$

也就是說 $g+pt$ 是模 p^α 的元根。

f. 設 $\alpha\geqslant 1$ 而且 g_1 是模 p^α 的元根，則数 g_1 和 g_1+p^α 中間的奇数是模 $2p^\alpha$ 的元根。

实际上，适合同余式 $x^\gamma\equiv 1 \pmod{p^\alpha}$ 和 $x^\gamma\equiv 1 \pmod{2p^\alpha}$ 中間一个的所有奇数 x，很明显地也适合另外一个。所以根据 $\varphi(p^\alpha)=$ $=\varphi(2p^\alpha)$，作为模 p^α 和 $2p^\alpha$ 中一个的元根的奇数 x，也是另外一个的元根。而在模 p^α 的元根 g_1 和 g_1+p^α 中間有一个是奇数；因此它就是模 $2p^\alpha$ 的元根。

§3. 模 p^α 和 $2p^\alpha$ 的元根的求法

設 p 是奇素数而且 $\alpha\geqslant 1$，則模 p^α 和 $2p^\alpha$ 的元根可以利用下面的普遍定理求得。

設 $c=\varphi(m)$ 而且 $q_1, q_2, \cdots, q_k$ 是 c 的不同的素約数。則与 m 互素的数目 g 是模 m 的元根的必要而且充分的条件是：这个 g 不适合下列同余式的任何一个：

$$g^{\frac{c}{q_1}}\equiv 1 \pmod{m},\quad g^{\frac{c}{q_2}}\equiv 1 \pmod{m},\ \cdots,\ g^{\frac{c}{q_k}}\equiv 1 \pmod{m}. \quad (1)$$

实际上，如果 g 是元根，則它就屬于方次数 c，因此(1)里的同余式就沒有一个成立。

反之，假設 g 不适合(1)里的任何一个同余式。如果 g 所屬的方次数 δ 小于 c，則用 q 表示 $\frac{c}{\delta}$ 的素約数的一个，我們有 $\frac{c}{\delta}=qu$，$\frac{c}{q}=\delta u$，$g^{\frac{c}{q}}\equiv 1 \pmod{p}$，与我們的假設矛盾。这說明 $\delta=c$，而 g 就是元根。

例子 1. 設 $m=41$，我們有 $\varphi(41)=40=2^3\cdot 5$，$\frac{40}{5}=8$，$\frac{40}{2}=$ $=20$。因此对于不被 41 除尽的数 g 說，它是模 41 的元根的必要而且充分的条件，是 g 不适合下列同余式的任何一个：

$$g^8\equiv 1 \pmod{41},\quad g^{20}\equiv 1 \pmod{41}. \qquad (2)$$

但是試驗 2, 3, 4, … 等数目，我們發現(对于模 41)

$$2^8\equiv30,\quad 3^8\equiv1,\quad 4^8\equiv18,\quad 5^8\equiv18,\quad 6^8\equiv10,$$
$$2^{20}\equiv1,\qquad\qquad 4^{20}\equiv1,\quad 5^{20}\equiv1,\quad 6^{20}\equiv40.$$

由此我們看到，2, 3, 4, 5 都不是元根，因为它們至少适合(2)式的一个。而 6 是元根，因为它不适合(2)式的任何一个。

例子 2. 設 $m=1681=41^2$。利用上面的普遍定理，我們能在这里求出元根。但应用 § 2, e 的定理，我們更容易求出它来。已經知道模 41 的一个元根是 6(例子 1)，我們看到

$$6^{40}=1+41(3+41l),$$
$$(6+41t)^{40}=1+41(3+41l-6^{39}t+41T)=1+41u.$$

要使 u 不被 p 除尽，只要取 $t=0$ 就成。所以我們可以取 $6+41\cdot0==6$ 作为模 1681 的元根。

例子 3. 設 $m=3362=2\cdot1681$。利用上面的定理，我們能在这里求出元根。但应用 § 2, f 的定理，我們更容易求出它来。已經知道模 1681 的一个元根是 6，我們可以取 6 和 6+1681 中間的奇数，也就是 1687，作为模 3362 的元根。

§ 4. 模 p^α 和 $2p^\alpha$ 的指数

a. 設 p 是奇素数，$\alpha\geqslant1$；m 是 p^α 和 $2p^\alpha$ 中間的一个；$c=\varphi(m)$，g 是模 m 的元根。

b. 如果 γ 通过模 c 的非負的最小剩余 $\gamma=0, 1, \cdots, c-1$。則 g^γ 通过与模 m 互素的剩余組。

实际上，g^γ 所通过的与 m 互素的 c 个数，根据 § 1, b，对于模 m 都不同余。

c. 对于与 m 互素的 a，我們可以引进与对数的概念类似的指数的概念；这时元根起着与对数的底数一样的作用。

如果 $$a\equiv g^\gamma\pmod m$$

(假設 $\gamma\geqslant 0$), 則 γ 就叫做 a 对于模 m 的以 g 为底的指数，用符号 $\gamma=\operatorname{ind} a$(更正确地 $\gamma=\operatorname{ind}_g a$)来表示。

根据 b, 每一个与 m 互素的 a, 都有唯一的一个指数 γ' 出現在下列数中間:

$$\gamma'=0, 1, \cdots, c-1.$$

知道了 γ', 我們能求得 a 的所有指数; 按照 § 1, c, 它們就是下列数类里所有非負的数:

$$\gamma\equiv\gamma'(\bmod c).$$

从指数的定义可以直接推出: 有已知指数 γ 的数組成模 m 的一个数类。

d. 我們有

$$\operatorname{ind} ab\cdots l\equiv\operatorname{ind} a+\operatorname{ind} b+\cdots+\operatorname{ind} l(\bmod c),$$

特别地

$$\operatorname{ind} a^n\equiv n \operatorname{ind} a(\bmod c).$$

实际上,

$$a\equiv g^{\operatorname{ind} a}(\bmod m),\ b\equiv g^{\operatorname{ind} b}(\bmod m),\ \cdots,\ l\equiv g^{\operatorname{ind} l}(\bmod m),$$

于是把它們乘起来就有

$$ab\cdots l\equiv g^{\operatorname{ind} a+\operatorname{ind} b+\cdots+\operatorname{ind} l}(\bmod m).$$

因此, $\operatorname{ind} a+\operatorname{ind} b+\cdots+\operatorname{ind} l$ 是乘积 $ab\cdots l$ 的一个指数。

e. 为了指数的实用的便利，对于每个素数模 p(自然是不太大的), 我們造出指数表来。这是兩个表: 一个是从数求出指数, 另外一个是从指数求出数。表中包括数对于模 p 的非負的最小剩余(与模互素的剩余組)和它們对于模 $c=\varphi(p)=p-1$ 的最小的指数(完全剩余組)。

例子 讓我們来造出模 $p=41$ 的表, 前面(§ 3, 例子 1)曾經指出过 $g=6$ 是模 41 的元根; 我們拿它来作指数的底。求出(同余式

都取模 41)：

$6^0\equiv1$	$6^8\equiv10$	$6^{16}\equiv18$	$6^{24}\equiv16$	$6^{32}\equiv37$
$6^1\equiv6$	$6^9\equiv19$	$6^{17}\equiv26$	$6^{25}\equiv14$	$6^{33}\equiv17$
$6^2\equiv36$	$6^{10}\equiv32$	$6^{18}\equiv33$	$6^{26}\equiv2$	$6^{34}\equiv20$
$6^3\equiv11$	$6^{11}\equiv28$	$6^{19}\equiv34$	$6^{27}\equiv12$	$6^{35}\equiv38$
$6^4\equiv25$	$6^{12}\equiv4$	$6^{20}\equiv40$	$6^{28}\equiv31$	$6^{36}\equiv23$
$6^5\equiv27$	$6^{13}\equiv24$	$6^{21}\equiv35$	$6^{29}\equiv22$	$6^{37}\equiv15$
$6^6\equiv39$	$6^{14}\equiv21$	$6^{22}\equiv5$	$6^{30}\equiv9$	$6^{38}\equiv8$
$6^7\equiv29$	$6^{15}\equiv3$	$6^{23}\equiv30$	$6^{31}\equiv13$	$6^{39}\equiv7$

所以所求的表是：

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

这里横列的号碼表示数(或指数)的十位数，直行的号碼則表示个位数。而在圖表中处于某一横列和某一直行的公共部分的就是对应的指数(或数)。

例如,要求 ind 25, 从第一个表里找号碼 2 的横列和号碼 5 的直行的公共部分,也就是 ind 25 = 4。而要求有指数 33 的数,从第二个表里找号碼 3 的横列和号碼 3 的直行的公共部分，也就是 33 = ind 17。

§ 5. 前面理論的一些推論

a. 設 p 是奇素数；$\alpha\geqslant1$，m 是p^α 和 $2p^\alpha$ 中間的一个。最后，

設 $c=\varphi(m)$。

b. 設$(n, c)=d$; 那末:

1. 同余式

$$x^n \equiv a \pmod{m} \quad (1)$$

能解(因而 a 是模 m 的 n 次剩余), 在而且只在 ind a 是 d 的倍数时。

在可解的情形下,同余式(1)有 d 个解答。

2. 在与模 m 互素的剩余中間, n 次剩余的个数是 $\frac{c}{d}$。

实际上,同余式(1)等价于同余式

$$n \text{ ind } x \equiv \text{ind } a \pmod{c}, \quad (2)$$

后者能解在而且只在 ind a 是 d 的倍数时(第四章 § 2, d)。

在同余式(2)可解的情形下,我們能找出对于模 c 不同余的 d 个 ind x; 与它們对应的是对于模 m 不同余的 d 个 x。

因此命題 1 正确。

作为与模 m 互素的剩余組里剩余的最小指数, 在数 $0, 1, \cdots, c-1$ 中間有 $\frac{c}{d}$ 个是 d 的倍数。所以命題 2 是正确的。

例子 1. 对于同余式

$$x^8 \equiv 23 \pmod{41}, \quad (3)$$

我們有$(8, 40)=8$, 幷且 ind $23=36$ 不被 8 除尽, 所以同余式(3)不能解。

例子 2. 对于同余式

$$x^{12} \equiv 37 \pmod{41}, \quad (4)$$

我們有$(12, 40)=4$, 幷且 ind $37=32$ 能被 4 除尽。所以同余式(4)能解,幷且它有 4 个解答。我們用下面的方法来求这些解答。

同余式(4)等价于同余式

$$12 \text{ ind } x \equiv 32 \pmod{40}, \text{ ind } x \equiv 6 \pmod{10}.$$

由此我們求得 4 个对于模 40 不同余的 ind x 的値

$$\text{ind}\, x = 6, 16, 26, 36,$$

对应地我們求得同余式(4)的 4 个解答

$$x \equiv 39, 18, 2, 23 \pmod{41}.$$

例子 3. 数

$$1,\ 4,\ 10,\ 16,\ 18,\ 23,\ 25,\ 31,\ 37,\ 40 \qquad (5)$$

的指数都是 4 的倍数，这些数正好是模 41 的最小正剩余中間的全部四次剩余（也是次数 $n=12, 28, 36, \cdots$ 这里 $(n, 40)=4$ 的剩余）。数列(5)的数个数是 $10=\frac{40}{4}$。

c. 与 b 的命題 1 同时，便于利用的还有：

数 a 是 n 次剩余，如果而且只如果

$$a^{\frac{c}{d}} \equiv 1 \pmod{m}. \qquad (6)$$

实际上，条件 ind $a \equiv 0 \pmod{d}$ 与 $\frac{c}{d}$ ind $a \equiv 0 \pmod{c}$ 等价。而后者又与条件(6)等价。

例子 在 § 3 的定理中，同余式 $g^{\frac{c}{q}} \equiv 1 \pmod{m}$ 不成立与 g 是模 m 的 q 次非剩余等价。特别地，同余式 $g^{\frac{c}{2}} \equiv 1 \pmod{m}$ 不成立与 g 是模 m 的平方非剩余等价(参看第五章 § 1, e)。

d, 1. a 对于模 m 所屬的方次数 δ，由等式 $(\text{ind}\, a, c) = \frac{c}{\delta}$ 确定；特别地，a 是模 m 的元根由等式 $(\text{ind}\, a, c) = 1$ 确定。

2. 在与模 m 互素的剩余組中，屬于方次数 δ 的数的个数是 $\varphi(\delta)$；特别地，元根的个数是 $\varphi(c)$。

实际上，δ 是有条件 $a^{\delta} \equiv 1 \pmod{m}$ 的 c 的最小約数。这条件等价于

$$\delta\, \text{ind}\, a \equiv 0 \pmod{c}$$

或者
$$\operatorname{ind} a \equiv 0\left(\bmod \frac{c}{\delta}\right).$$

这說明，δ 是使 $\frac{c}{\delta}$ 除尽 ind a 的 c 的最小約数，因此 $\frac{c}{\delta}$ 是除尽 ind a 的 c 的最大約数，这就是說 $\frac{c}{\delta}=(\operatorname{ind} a, c)$。所以命題 1 是正确的。

在与模 m 互素的剩余組里剩余的最小指数 $0, 1, \cdots, c-1$ 中間，$\frac{c}{\delta}$ 的倍数有形式 $\frac{c}{\delta}y$，这里 $y=0, 1, \cdots, \delta-1$。条件 $\left(\frac{c}{\delta}y, c\right)=\frac{c}{\delta}$ 与 $(y, \delta)=1$ 等价；后者被 $\varphi(\delta)$ 个 y 所适合。所以命題 2 是正确的。

例子 1. 在与模 41 互素的剩余組中，屬于方次数 10 的数 a，乃是适合条件 $(\operatorname{ind} a, 40)=\frac{40}{10}=4$ 的，也就是

$$4,\ 23,\ 25,\ 31.$$

这些数的个数是 $4=\varphi(10)$。

例子 2. 在与模 41 互素的剩余組中，元根乃是适合条件 $(\operatorname{ind} a, 40)=1$ 的数 a，也就是

$$6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.$$

这些元根的个数是 $16=\varphi(40)$。

§ 6. 模 2^α 的指数

a. 对于模 2^α，上面的定理都要由一些更复杂的来代替。

b. 設 $\alpha=1$。那末 $2^\alpha=2$。我們有 $\varphi(2)=1$。模 2 的元根是，例如 $1\equiv-1 \pmod 2$。数 $1^0=(-1)^0=1$ 就組成与模 2 互素的剩余組。

c. 設 $\alpha=2$。那末 $2^\alpha=4$。我們有 $\varphi(4)=2$。模 4 的元根是，例如 $3\equiv-1 \pmod 4$。数 $(-1)^0=1, (-1)^1\equiv 3 \pmod 4$ 組成与模

4 互素的剩余組。

d. 設 $\alpha\geqslant 3$。那末 $2^\alpha\geqslant 8$。我們有 $\varphi(2^\alpha)=2^{\alpha-1}$。不难看到，在这个情形下是沒有元根的；更正确地說：对于模 2^α，單数 x 所屬的方次数不能超过 $2^{\alpha-2}=\frac{1}{2}\varphi(2^\alpha)$。实际上，我們有

$$x^2=1+8t_1,$$
$$x^4=1+16t_2,$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$x^{2^{\alpha-2}}=1+2^\alpha t_{\alpha-2}\equiv 1 \pmod{2^\alpha}.$$

这时屬于方次数 $2^{\alpha-2}$ 的数一定存在。例如 5 就是这样的一个数。实际上

$$5=1+4,$$
$$5^2=1+8+16,$$
$$5^4=1+16+32u_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$5^{2^{\alpha-3}}=1+2^{\alpha-1}+2^\alpha u_{\alpha-3},$$

于是我們看到，乘幂 $5^1, 5^2, 5^4, \cdots, 5^{2^{\alpha-3}}$ 中間沒有一个对于模 2^α 与 1 同余。

不难看到，下面的兩排数：

$$5^0, 5^1, \cdots, 5^{2^{\alpha-2}-1},$$

$$-5^0, -5^1, \cdots, -5^{2^{\alpha-2}-1},$$

組成与模 2^α 互素的剩余組。实际上，这些数的个数正好是 $2\cdot 2^{\alpha-2}=\varphi(2^\alpha)$；同一排的数对于模 2^α 都不同余（§ 1, b）；而且上一排的数与下一排的数也不同余，因为对于模 4，第一个与 1 同余而第二个却与 -1 同余。

e. 为了进一步討論的方便，我們把 b, c 和 d 里的結果放到一个統一的形式里去。这形式就是对于 $\alpha=0$ 的情形也能适合。

設 $c=1; c_0=1$, 如果 $\alpha=0$ 或者 $\alpha=1$;

$c=2; c_0=2^{\alpha-2}$, 如果 $\alpha\geqslant 2$。

(这样一来总有 $cc_0=\varphi(2^\alpha)$)。再設 γ 和 γ_0 互相独立地通过模 c 和 c_0 的非負的最小剩余

$$\gamma=0, \cdots, c-1; \quad \gamma_0=0, \cdots, c_0-1.$$

那末 $(-1)^\gamma 5^{\gamma_0}$ 通过与模 2^α 互素的剩余組。

f. 同余式

$$(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} \pmod{2^\alpha} \qquad (1)$$

成立，如果而且只如果

$$\gamma\equiv\gamma' \pmod{c}, \quad \gamma_0\equiv\gamma_0' \pmod{c_0}.$$

实际上，当 $\alpha=0$, 定理是显然的。所以我們可以假定 $\alpha>0$。設数 γ 和 γ_0 对于模 c 和 c_0 的非負的最小剩余是 r 和 r_0, 而数 γ' 和 γ_0' 的则是 r' 和 r_0'。根据 §1, c(-1 屬于方次数 c, 而 5 屬于方次数 c_0), 同余式 (1) 成立如果而且只如果 $(-1)^r 5^{r_0}\equiv(-1)^{r'} 5^{r_0'}\cdot$ $\pmod{2^\alpha}$, 也就是(根据 e) $r=r'$, $r_0=r_0'$。

g. 如果 $a\equiv(-1)^\gamma 5^{\gamma_0} \pmod{2^\alpha}$,

則組 γ, γ_0 叫做数 a 对于模 2^α 的指数組。

根据 e, 每一个与 2^α 互素(也就是奇数)的 a, 总有唯一的一組指数 γ', γ_0' 在 $cc_0=\varphi(2^\alpha)$ 对 γ, γ_0 中間。

知道了一組 γ', γ_0', 我們能求得 a 的所有指数組；根据f, 它們就是由下列数类中的非負的数所組成的各对 γ, γ_0。

$$\gamma\equiv\gamma' \pmod{c}, \quad \gamma_0\equiv\gamma_0' \pmod{c_0}.$$

直接从这个关于指数組的定义推出，有已知指数組 γ, γ_0 的所有的数，組成模 2^α 的一个数类。

h. 乘积的指数，对于模 c 和 c_0，与各个因子的指数的总和同余。

实际上，設 $\gamma(a)$, $\gamma_0(a)$, $\cdots$; $\gamma(l)$, $\gamma_0(l)$ 是数 $a, \cdots, l$ 的指数組。我們有

$$a\cdots l \equiv (-1)^{\gamma(a)+\cdots+\gamma(l)} 5^{\gamma_0(a)+\cdots+\gamma_0(l)}.$$

因此，$\gamma(a)+\cdots+\gamma(l)$, $\gamma_0(a)+\cdots+\gamma_0(l)$是乘积 $a\cdots l$ 的指数組。

§7. 任意复合数模的指数

a. 設 $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 是数 m 的标准分解式。再設 c 和 c_0 有 §6, e 里所說的值；$c_s=\varphi\left(p_s^{\alpha_s}\right)$；$g_s$ 是模 $p_s^{\alpha_s}$ 的最小的元根。

b. 如果

$$\left.\begin{aligned} &a\equiv(-1)^{\gamma}5^{\gamma_0}(\bmod 2^{\alpha}),\\ &a\equiv g_1^{\gamma_1}(\bmod p_1^{\alpha_1}), \cdots, a\equiv g_k^{\gamma_k}(\bmod p_k^{\alpha_k}),\end{aligned}\right\} \tag{1}$$

則 $\gamma, \gamma_0, \gamma_1, \cdots, \gamma_k$ 叫做 a 对于模 m 的指数組。

从这个定义推出，γ, γ_0 是 a 对于模 2^{α} 的指数組，而 $\gamma_1, \cdots, \gamma_k$ 分别是 a 对于模 $p_1^{\alpha_1}, \cdots, p_k^{\alpha_k}$ 的指数。所以与 m 互素的每一个 a（它也与所有的 $2^{\alpha}, p_1^{\alpha_1}, \cdots, p_k^{\alpha_k}$ 互素）有唯一的一組指数 γ', γ_0', $\gamma_1', \cdots, \gamma_k'$ 在 $cc_0c_1\cdots c_k=\varphi(m)$ 个組 γ, γ_0, $\gamma_1, \cdots$, γ_k 中間（§6, g, §4, c）。讓 $\gamma, \gamma_0, \gamma_1, \cdots, \gamma_k$ 独立地通过模 $c, c_0, c_1, \cdots, c_k$ 的非負的最小剩余組，就得到这 $\varphi(m)$个組。而且 a 的所有指数組，可以由下列数类中非負的数 $\gamma, \gamma_0, \gamma_1, \cdots, \gamma_k$ 組成：

$$\gamma\equiv\gamma'(\bmod c),\ \gamma_0\equiv\gamma_0'(\bmod c_0),$$
$$\gamma_1\equiv\gamma_1'(\bmod c_1),\ \cdots,\ \gamma_k\equiv\gamma_k'(\bmod c_k).$$

有已知指数組 $\gamma, \gamma_0, \gamma_1, \cdots, \gamma_k$ 的数 a，可以从解同余式組（1）求得，因此就組成模 m 的数类（第四章 §3, b）。

c. 因为 a 对于模 m 的指数 $\gamma, \gamma_0, \gamma_1, \cdots, \gamma_k$, 分别是它对于模 $2^\alpha, p_1^{\alpha_1}, \cdots, p_k^{\alpha_k}$ 的指数，所以下列定理眞实。

乘积的指数，对于模 $cc_0c_1\cdots c_k$，与它的因子的指数的总和同余。

d. 設 $\tau=\varphi(2^\alpha)$ 当 $\alpha\leqslant 2$, 而 $\tau=\frac{1}{2}\varphi(2^\alpha)$ 当 $\alpha>2$。再設 h 是数 $\tau, c_1, \cdots, c_k$ 的最小公倍数。对于每个与 m 互素的 a, 同余式 $a^h\equiv 1$ 对于所有的模 $2^\alpha, p_1^{\alpha_1}, \cdots, p_k^{\alpha_k}$ 都成立，这說明这个同余式对于模 m 也成立。所以当 $h<\varphi(m)$ 时，a 不能是模 m 的元根。但是当 $\alpha>2$ 时，当 $k>1$ 时，以及当 $\alpha=2, k=1$ 时，都有 $h<\varphi(m)$ 成立。所以对于 $m>1$, 只有在 $m=2, 4, p_1^{\alpha_1}, 2p_1^{\alpha_1}$ 的情形下，才可能有元根存在。但是在这些情形下元根的存在已經証明(§2, §6)。所以

对于大于 1 的模 m，有元根存在的所有情形是

$$m=2, 4, p^\alpha, 2p^\alpha.$$

問　題

以下 p 总表示奇素数，但在問題 11, b 里也表示 2。

1, a. 設 a 是整数，$a>1$。証明，a^p-1 的奇素約数不是除尽 $a-1$, 就是有形式 $2px+1$。

b. 設 a 是整数，$a>1$。証明，a^p+1 的奇素約数不是除尽 $a+1$, 就是有形式 $2px+1$。

c. 証明形式 $2px+1$ 的素数的个数是無限的。

d. 設 n 是整数，$n>0$。証明，$2^{2^n}+1$ 的約数有形式 $2^{n+1}x+1$。

2. 設 a 是整数，$a>1$, n 是整数，$n>0$。証明 $\varphi(a^n-1)$ 是 n 的倍数。

3, a. 設 n 是整数，$n>1$。当 n 是奇数时，从数 $1, 2, \cdots, n$ 作成排列

$$1, 3, 5, \cdots, n-2, n, n-1, n-3, \cdots, 4, 2;$$

$$1, 5, 9, \cdots 7, 3;$$

等等。而当 n 是偶数时，则作成排列

$$1, 3, 5, \cdots, n-1, n, n-2, \cdots, 4, 2;$$

$$1, 5, 9, \cdots, 7, 3;$$

等等。証明，第 k 次这样的运算給出原来数列，在而且只在 $2^k \equiv \pm 1 \pmod{2n-1}$ 时。

b. 設 n 是整数，$n>1$，m 是整数，$m>1$。我們来数 $1, 2, \cdots\cdots, n$，先順的从 1 数到 n，再倒的从 n 数到 2，然后又順的从 1 数到 n，再倒的从 n 数到 2，等等。在这样的数法中写下第 1 个，第 $m+1$ 个，第 $2m+1$ 个等等的数，直到 n 个数都写出才止。对于这新的数列重新使用同样的运算，繼續下去。証明第 k 次这样的运算給出原先数列的必要而且充分的条件是

$$m^k \equiv \pm 1 \pmod{2n-1}.$$

4. 討論同余式 $x^\delta \equiv 1 \pmod{p}$ (第四章問題 10, c)，应用第二章 § 3, d，証明屬于方次数 δ 的数有 $\varphi(\delta)$ 个。

5, a. 証明 3 是形式 2^n+1, $n>1$ 的素数的元根。

b. 証明，形式 $2p+1$ 的素数，当 p 是 $4n+1$ 形式时，有元根 2，当 p 是 $4n+3$ 形式时，有元根 -2。

c. 証明 2 是 $4p+1$ 形式的素数的元根。

d. 証明 3 是下列形式的素数的元根

$$2^n p+1,\ n>1,\ p>\frac{3^{2^{n-1}}}{2^n}.$$

6, a, α) 設 n 是整数，$n>0$，$S=1^n+2^n+\cdots+(p-1)^n$。証明

$S \equiv -1 \pmod{p}$，如果 n 是 $p-1$ 的倍数，

$S\equiv 0 \pmod p$，其他情形。

β) 采用第五章問題 9, c 的記号，証明

$$S(1)\equiv -\begin{pmatrix}\frac{p-1}{2}\\ \frac{p-1}{4}\end{pmatrix} \pmod p.$$

b. 应用 § 4, b, 証明威尔逊定理。

7. 設 g 和 g_1 都是模 p 的元根，$\alpha\,\mathrm{ind}_g\, g_1\equiv 1 \pmod{p-1}$。

a. 設 $(a, p)=1$。証明

$$\mathrm{ind}_{g_1} a\equiv \alpha\,\mathrm{ind}_g a \pmod{p-1}.$$

b. 設 n 是 $p-1$ 的約数，$1<n<p-1$。与 p 互素的数可以分成 n 个集合，使得屬于第 s 个 $(s=0, 1, \cdots, n-1)$ 集合的数都适合条件 $\mathrm{ind}\, a\equiv s \pmod n$。証明，如果 $s_1\equiv \alpha s \pmod n$，則对于底数 g 有号碼 s 的集合，与对于底数 g_1 就有号碼 s_1 的集合全同。

8. 在模 p 的某个元根 g 已知的情形下，指出解同余式 $x^n\equiv a \pmod p$（不妨假定 $(n, p-1)$ 不太大）的最簡單的方法。

9. 設 $m, a, c, c_0, c_1, \cdots, c_k, \gamma, \gamma_0, \gamma_1, \cdots, \gamma_k$ 有 § 7 里所說的值。取方程

$$R^c=1,\ R_0^{c_0}=1,\ R_1^{c_1}=1, \cdots,\ R_k^{c_k}=1$$

的任意根 $R, R_0, R_1, \cdots, R_k$。假定

$$\chi(a)=R^{\gamma} R_0^{\gamma_0} R_1^{\gamma_1} \cdots R_k^{\gamma_k}.$$

而如果 $(a, m)>1$，則假定 $\chi(a)=0$。

用这样方法定出来的对于所有整数都有定义的函数，叫做品格函数。当 $R=R_0=R_1=\cdots=R_k=1$，它叫做主品格；它的值当 $(a, m)=1$ 时是 1，$(a, m)>1$ 时是 0。

a. 証明上述方法使我們能得到 $\varphi(m)$ 个不同的品格（兩个品

格說是不同的，如果它們至少对于一个 a 有不相等的値)。

b. 引出品格的下列性質：

α) $\chi(1)=1$.

β) $\chi(a_1a_2)=\chi(a_1)\chi(a_2)$.

γ) $\chi(a_1)=\chi(a_2)$，如果 $a_1\equiv a_2 \pmod m$。

c. 証明

$$\sum_{a=0}^{m-1}\chi(a)=\begin{cases}\varphi(m), & \text{对于主品格,}\\ 0, & \text{对于其他的品格。}\end{cases}$$

d. 証明，对于已知的 a 取所有 $\varphi(m)$ 个品格的总和，我們有

$$\sum_{\chi}\chi(a)=\begin{cases}\varphi(m), & \text{如果 } a\equiv 1 \pmod m,\\ 0, & \text{其他情形。}\end{cases}$$

e. 設函数 $\psi(a)$ 对于所有整数 a 都有定义，而且适合条件

$\psi(a)=0$，如果 $(a, m)>1$，

$\psi(a)$ 不恒等于 0，

$\psi(a_1a_2)=\psi(a_1)\psi(a_2)$，

$\psi(a_1)=\psi(a_2)$，如果 $a_1\equiv a_2 \pmod m$。

討論和式

$$H=\sum_{\chi}\sum_{a}\frac{\chi(a)}{\psi(a)},$$

証明 $\psi(a)$ 是一个品格。

f. 証明下面的定理：

α) 如果 $\chi_1(a)$ 和 $\chi_2(a)$ 都是品格，則 $\chi_1(a)\chi_2(a)$ 也是品格。

β) 如果 $\chi_1(a)$ 是一个品格，而且 $\chi(a)$ 通过所有的品格，則 $\chi_1(a)\chi(a)$ 也通过所有的品格。

γ) 当 $(l, m)=1$ 时；我們有

$$\sum_{\chi}\frac{\chi(a)}{\chi(l)}=\begin{cases}\varphi(m), & 如果\ a\equiv l(\operatorname{mod} m),\\ 0, & 其他情形。\end{cases}$$

10, a. 設 n 是 $p-1$ 的約数，$1<n\leqslant p-1$, l 是整数，不被 n 除尽。数 $R_1=e^{2\pi i\frac{l}{n}}$ 是方程 $R_1^n=1$ 的根，因此 $e^{2\pi i\frac{l\operatorname{ind} x}{n}}$（当 x 是 p 的倍数时，它等于 0）是模 p 的品格。

α) 当 $(k,p)=1$ 时，証明

$$\sum_{x=1}^{p-1}e^{2\pi i\frac{l\operatorname{ind}(x+k)-l\operatorname{ind}x}{n}}=-1.$$

β) 設 Q 是整数，$1<Q<p$,

$$S=\sum_{x=0}^{p-1}|S_{l,n,x}|^2;\ S_{l,n,x}=\sum_{z=0}^{Q-1}e^{2\pi i\frac{l\operatorname{ind}(x+z)}{n}}.$$

証明
$$S=(p-Q)Q.$$

γ) 設 $p>4n^2$, $n>2$, M 是整数。証明在数列 $M, M+1, \cdots, M+2[n\sqrt{p}]-1$ 中間有屬于問題 7, b 里第 s 个集合的数。

b. 設 $p>4\left(\frac{p-1}{\varphi(p-1)}\right)^2 2^{2k}$, k 是 $p-1$ 的不同的素約数的个数，M 是整数。証明，在数列

$$M, M+1, \cdots, M+2\left[\frac{p-1}{\varphi(p-1)}2^k\sqrt{p}\right]-1$$

中間有模 p 的元根。

11, a. 設 a 是整数，n 是 $p-1$ 的約数，$1<n\leqslant p-1$, k 是不被 n 除尽的整数，

$$U_{a,p}=\sum_{x=1}^{p-1}e^{2\pi i\frac{k\operatorname{ind}x}{n}}e^{2\pi i\frac{ax}{p}},$$

α) 当$(a, p)=1$时，証明

$$|U_{a,p}|=\sqrt{p}.$$

β) 証明

$$e^{2\pi i\frac{-k\operatorname{ind}a}{n}}=\frac{U_{a,p}}{U_{1,p}}.$$

γ) 設p有形式$4m+1$,

$$S=\sum_{x=1}^{p-2}e^{2\pi i\frac{\operatorname{ind}(x^2+x)}{4}}.$$

証明$p=A^2+B^2$, 这里A和B都是整数，由等式$S=A+Bi$定出(参看第五章問題9, a和9, c)。

b. 設n是整数,$n>2, m>1, (a, m)=1$,

$$S_{a,m}=\sum_{x}e^{2\pi i\frac{ax^n}{m}},\quad S'_{a,m}=\sum_{\xi}{}'e^{2\pi i\frac{a\xi^n}{m}},$$

这里x和ξ分别通过模m的完全剩余組和与模互素的剩余組(参看第三章問題12, d和第五章問題11, b)。

α) 設$\delta=(n, p-1)$。証明

$$|S_{a,p}|\leqslant(\delta-1)\sqrt{p}.$$

β) 設$(n, p)=1$, s是整数，$1<s\leqslant n$。証明

$$S_{a,p^s}=p^{s-1},\quad S'_{a,p^s}=0.$$

γ) 設s是整数，$s>n$。証明

$$S_{a,p^s}=p^{n-1}S_{a,p^{s-n}},\quad S'_{a,p^s}=0.$$

δ) 証明

$$|S_{a,m}|<Cm^{1-\frac{1}{n}},$$

这里C只与n有关。

12. 設M和Q都是整数，$0<M<M+Q\leqslant p$。

a. 設 n 是 $p-1$ 的約数，$1<n<p-1$，k 是不被 n 除尽的整数。証明

$$\left|\sum_{x=M}^{M+Q-1} e^{2\pi i\frac{k\,\mathrm{ind}\,x}{n}}\right|<\sqrt{p}\ln p.$$

b. 設 T 是問題 7, b 里第 s 个集合里的数出現在数 M, $M+1, \cdots, M+Q-1$ 中間的个数。証明

$$T=\frac{Q}{n}+\theta\sqrt{p}\ln p;\quad |\theta|<1.$$

c. 設 k 是 $p-1$ 的素約数的个数，H 是模 p 的元根出現在数 $M, M+1, \cdots, M+Q-1$ 中間的个数。証明

$$H=\frac{\varphi(p-1)}{p-1}Q+\theta 2^k\sqrt{p}\ln p;\quad |\theta|<1.$$

d. 設 M_1 和 Q_1 都是整数，$0\leqslant M_1<M_1+Q\leqslant p-1$，$J$ 是数列 $\mathrm{ind}\,M$, $\mathrm{ind}(M+1), \cdots, \mathrm{ind}(M+Q-1)$ 里的数出現在数列 M_1, $M_1+1, \cdots, M_1+Q-1$ 中間的个数。証明

$$J=\frac{QQ_1}{p-1}+\theta\sqrt{p}(\ln p)^2;\quad |\theta|<1.$$

13. 証明适合下面条件的常数 p_0 的存在：如果 $p>p_0$，n 是 $p-1$ 的約数，$1<n<p-1$，則模 p 的 n 次非剩余中最小的正数

$$<h;\quad h=p^{\frac{1}{c}}(\ln p)^2;\quad c=2e^{1-\frac{1}{n}}.$$

14, a. 設 $m>1$，$(a, m)=1$，

$$S=\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\nu(x)\rho(y)e^{2\pi i\frac{axy}{m}};\quad \sum_{x=0}^{m-1}|\nu(x)|^2=X$$

$$\sum_{y=0}^{m-1}|\rho(y)|^2=Y.$$

証明
$$|S|\leqslant\sqrt{XYm}.$$

b. α) 設 $m>1$, $(a,m)=1$, n 是整数, $n>0$, K 是同余式 $x^n\equiv 1 \pmod m$的解答的个数,

$$S=\sum_{x=1}^{m-1}\chi(x)e^{2\pi i\frac{ax^n}{m}}.$$

証明

$$|S|\leqslant K\sqrt{m}.$$

β) 設 ε 是正的任意常数。关于問題 α 里的 K, 当 n 是常数时, 証明

$$K=O(m^{\varepsilon}).$$

15, a. 設$(a,p)=(b,p)=1$, n 是整数, $|n|=n_1$, $0<n_1<p$,

$$S=\sum_{x=1}^{p-1}e^{2\pi i\frac{ax^n+bx}{p}}.$$

証明

$$|S|<\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}.$$

b. 設$(A,p)=1$, n 是整数, $|n|=n_1$, $0<n_1<p$, M_0 和 Q_0 都是整数, $0<M_0<M_0+Q_0\leqslant p$。

α) 設

$$S=\sum_{x=M_0}^{M_0+Q_0-1}e^{2\pi i\frac{Ax^n}{p}}.$$

証明

$$|S|<\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}\ln p.$$

β) 設 M 和 Q 都是整数, $0<M<M+Q\leqslant p$。T 是数列 Ax^n; $x=M_0, M_0+1, \cdots, M_0+Q_0+1$ 中对于模 p 与数 $M, M+1, \cdots, M+Q-1$ 同余的数的个数。証明

$$T=\frac{Q_0Q}{p}+\theta\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}(\ln p)^2;\ |\theta|<1.$$

c. 設$(a, p)=1$, b 和 c 都是整数，$(b^2-4ac, p)=1$。

α) 設 γ 是整数

$$S=\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)e^{2\pi i\frac{\gamma x}{p}}.$$

証明

$$|S|<\frac{3}{2}p^{\frac{3}{4}}.$$

β) 設 M 和 Q 都是整数，$0<M<M+Q\leqslant p$,

$$S=\sum_{x=M}^{M+Q-1}\left(\frac{ax^2+bx+c}{p}\right).$$

証明

$$|S|<\frac{3}{2}p^{\frac{3}{4}}\ln p.$$

計 算 題

1, a. 用尽可能簡單的計算方法求 7 对于模 43 所屬的方次数。

b. 求 5 对于模 108 所屬的方次数。

2, a. 求模 17, 289, 578 的元根。

b. 求模 23, 529, 1058 的元根。

c. 求模 242 的最小元根。

3, a. 造出模 17 的指数表来。

b. 造出模 23 的指数表来。

4, a. 应用§5, c 的例子的説明求模 71 的元根。

b. 求模 191 的元根。

5, a. 利用指数表，指出下列同余式的解答的个数:

α) $x^{60}\equiv 79 \pmod{97}$.

β) $x^{55}\equiv17 \pmod{97}$.

γ) $x^{15}\equiv46 \pmod{97}$.

b. 指出下列同余式的解答的个数:

α) $3x^{12}\equiv31 \pmod{41}$.

β) $7x^{7}\equiv11 \pmod{41}$.

γ) $5x^{30}\equiv37 \pmod{41}$.

6, a. 利用指数表,解同余式:

α) $x^{2}\equiv59 \pmod{67}$.

β) $x^{35}\equiv17 \pmod{67}$.

γ) $x^{30}\equiv14 \pmod{67}$.

b. 解同余式:

α) $23x^{5}\equiv15 \pmod{73}$.

β) $37x^{6}\equiv69 \pmod{73}$.

γ) $44x^{21}\equiv53 \pmod{73}$.

7, a. 利用 § 5, c 的定理,确定下列同余式的解答的个数:

α) $x^{3}\equiv2 \pmod{37}$.

β) $x^{16}\equiv10 \pmod{37}$.

b. 确定下列同余式的解答的个数:

α) $x^{5}\equiv3 \pmod{71}$.

β) $x^{21}\equiv5 \pmod{71}$.

8, a. 应用問題 5 的方法, 解下列同余式(在解第二个同余式时,使用这本書最后的元根表):

α) $x^{7}\equiv37 \pmod{101}$,

β) $x^{5}\equiv44 \pmod{101}$.

b. 解同余式 $x^{3}\equiv23 \pmod{109}$。

9, a. 利用指数表,在与模 19 互素的剩余組中指出:α)平方剩余, β)立方剩余。

b. 在与模 37 互素的剩余組中指出: α) 15 次剩余, β) 8 次剩余。

10, a. 在与模 43 互素的剩余組中指出: α)屬于方次数 6 的数, β)全部元根。

b. 在与模 61 互素的剩余組中指出: α)屬于方次数 10 的数, β)全部元根。

問題解答

第一章

1. $ax+by$ 被 d 除所得的余数，还有形式 $ax'+by'$ 而且小于 d，就必需等于零。所以 d 除尽所有形式 $ax+by$ 的数。特別地，它同时除尽数 $a\cdot 1+b\cdot 0=a$ 和 $a\cdot 0+b\cdot 0=b$。另一方面，d 的表示式指出 a 和 b 的每一个公約数都除尽 d。所以 $d=(a, b)$。这样一来，§2, **d** 的定理也証明了。至于 §2, **e** 的定理可以这样得到：形式 $amx+bmy$ 的最小数是 amx_0+bmy_0；而形式 $\frac{a}{\delta}x+\frac{b}{\delta}y$ 的最小数则是 $\frac{a}{\delta}x_0+\frac{b}{\delta}y_0$。

这些結果的推广显然是对的。

2. 我們先注意到，两个不等的有理分数 $\frac{k}{l}$ 和 $\frac{m}{n}$ $(l>0,\ n>0)$ 中間的差数 $\geqslant\frac{1}{ln}$。不妨假定 $\delta_s<\delta_{s+1}$。設不等于 δ_s 的不可約分数 $\frac{a}{l}$ 有条件 $0<b\leqslant Q_s$。我們不可以有 $\delta_s<\frac{a}{b}<\delta_{s+1}$，否則就会有下面的矛盾情形：

$$\frac{a}{b}-\delta_s\geqslant\frac{1}{bQ_s},$$

$$\delta_{s+1}-\frac{a}{b}\geqslant\frac{1}{bQ_{s+1}},$$

$$\delta_{s+1}-\delta_s>\frac{1}{Q_sQ_{s+1}}.$$

所以 $\frac{a}{b}<\delta_s$ 或者 $\delta_{s+1}<\frac{a}{b}$。在这两种情形下 δ_s 都比 $\frac{a}{b}$ 更接近 α。

3. 当 $n\leqslant 6$ 时，定理是显然的；所以我們可以假定 $n>6$。于是就有

$$\xi=\frac{1+\sqrt{5}}{2}=1.618\cdots;\ \log_{10}\xi=0.2\cdots;$$

$$Q_2\geqslant 1=g_1=1,$$
$$Q_3\geqslant Q_2+1\geqslant g_2=2>\xi,$$
$$Q_4\geqslant Q_3+Q_2\geqslant g_3=g_2+g_1>\xi+1=\xi^2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$Q_n\geqslant Q_{n-1}+Q_{n-2}\geqslant g_{n-1}=g_{n-2}+g_{n-3}>\xi^{n-3}+\xi^{n-4}=\xi^{n-2}.$$

由此 $\quad N>\xi^{n-2};\ n<\dfrac{\log_{10}N}{\log_{10}\xi}+2<5k+2;\ n\leqslant 5k+1.$

4, a. 对于分数 $\frac{0}{1}$ 和 $\frac{1}{1}$ 我們有 $0\cdot 1-1\cdot 1=-1$。在有条件 $AD-BC=-1$ 的分数 $\frac{A}{B}$ 和 $\frac{C}{D}$ 中間插进分数 $\frac{A+C}{B+D}$，我們有 $A(B+D)-B(A+C)=(A+C)D-(B+D)C=-1$。所以在問題最后所提出的断言是对的。适合条件 $\frac{a}{b}<\frac{k}{l}<\frac{c}{d}$，$l<\tau$ 的分数 $\frac{k}{l}$ 不可能存在。否則我們就会有

$$\frac{k}{l}-\frac{a}{b}\geqslant\frac{1}{lb};\quad \frac{c}{d}-\frac{k}{l}\geqslant\frac{1}{ld};\quad \frac{c}{d}-\frac{a}{b}\geqslant\frac{b+d}{lbd}>\frac{1}{bd}.$$

b. 明显地，只要討論 $0\leqslant\alpha<1$ 的情形就够了。設 $\frac{a}{b}\leqslant\alpha<\frac{c}{d}$，这里 $\frac{a}{b}$ 和 $\frac{c}{d}$ 是与 τ 对应的法雷級数中鄰接的分数。只可能有兩种情形：

$$\frac{a}{b}\leqslant\alpha<\frac{a+c}{b+d};\quad \frac{a+c}{b+d}\leqslant\alpha<\frac{c}{d}.$$

所以下列兩个不等式一定有一个成立：

$$\left|\alpha-\frac{a}{b}\right|<\frac{1}{b(b+d)};\quad \left|\alpha-\frac{c}{d}\right|\leqslant\frac{1}{d(b+d)}.$$

于是根据 $b+d>\tau$, 所說的定理立刻可以推出。

c. 当 α 是無理数时,如果取作 $\frac{P}{Q}$ 的是近似分数 $\frac{P_{s-1}}{Q_{s-1}}$, 这里 $Q_{s-1}\leqslant\tau<Q_s$, 定理可以从 § 4, h 推出。在 $\alpha=\frac{a}{b}$ 是有理数的情形里，上面的証明只适合于 $b>\tau$ 时。但是当 $b\leqslant\tau$ 时定理也是对的，因为这时只要讓 $\theta=0$, $\frac{P}{Q}$ 可以由分数 $\frac{a}{b}$ 本身来表示。

5, a. 奇素数被 4 除給出余数 1 或者 3。形式 $4m+1$ 的数的乘积还有形式 $4m+1$。所以設 $p_1, \cdots, p_k$ 都是形式 $4m+3$ 的素数，則数 $4p_1\cdots p_k-1$ 一定有形式 $4m+3$ 的素約数 q, 而这个 q 不等于 $p_1, \cdots p_k$ 中間的任何一个。

b. 大于 3 的素数都有形式 $6m+1$ 或者 $6m+5$。設 $p_1, \cdots, p_k$ 都是形式 $6m+5$ 的素数，則数 $6p_1\cdots p_k-1$ 一定有形式 $6m+5$ 的素約数 q, 而这个 q 不等于 $p_1, \cdots, p_k$ 中間的任意一个。

6. 設 $p_1, \cdots, p_k$ 是任意 k 个素数，N 是整数有条件 $2<N$, $(3\ln N)^k<N$。在数列 $1, 2, \cdots, N$ 中間有标准分解式 $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 的数 a 的个数,由于 $\alpha_s\leqslant\frac{\ln N}{\ln 2}$, 就

$$\leqslant\left(\frac{\ln N}{\ln 2}+1\right)^k<(3\ln N)^k<N.$$

所以在数列 $1, 2, \cdots, N$ 中能找到数,在它的标准分解式中除掉 $p_1, \cdots, p_k$ 以外还有别的素数。

7. 例如,当

$$M=2\cdot 3\cdots(K+1)t+2;\quad t=1, 2, \cdots,$$

我們就得到所求的数列。

8. 取整数 x_0 适合下面的条件：当 $x\geqslant x_0$ 时 $f(x)>1$, 而且 $f'(x)>0$。假設 $f(x_0)=X$。則所有的数 $f(x_0+Xt)$; $t=1, 2, \cdots$, 都是复合数(X 的倍数)。

9, a. (1)式中的 x, y 一定有一个(例如 x)是偶数; 从

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2},$$

这里显然有$\left(\frac{z+y}{2},\ \frac{z-y}{2}\right)=1$，可以肯定有正整数$u$和$v$存在，适合条件：

$$\frac{x}{2}=uv,\ \ \frac{z+y}{2}=u^2,\ \ \frac{z-y}{2}=v^2.$$

由此推出問題里所說的条件的必要性。

这些条件的充分性是很明显的。

b. 我們約定下面的字母只表示正整数。假設适合条件$x^4+y^4=z^2, x>0, y>0, z>0, (x, y, z)=1$的組$x, y, z$已經有了。从其中选擇有最小的$z$的組。假設$x$是偶数，我們得出$x^2=2uv$，$y^2=u^2-v^2, u>v\geqslant1, (u, v)=1$，这里$v$是偶数（如果$u$是偶数，則$y^2=4N+1, u^2=4N_1, v^2=4N_2+1, 4N+1=4N_1-4N_2-1$，这是不可能的）。由此$u=z_1^2,\ v=2w^2, y^2+4w^4=z_1^4,\ 2w^2=2u_1v_1,\ u_1=x_1^2$，$v_1=y_1^2, x_1^4+y_1^4=z_1^2$，由于$z_1<z$，这是不可能的。

从方程$x^4+y^4=z^2$的不可解性，作为特别情形，显然就推出方程$x^4+y^4=t^4$也沒有正整数x, y, t的解答。

10. 假設$x=\frac{k}{l}$；$(h, l)=1$，我們得出

$$k^n+a_1k^{n-1}l+\cdots+a_nl^n=0.$$

所以k^n是l的倍数，因此$l=1$。

11, a. 設k是适合条件$2^k\leqslant n$的最大整数，而P是所有不大于n的單数的乘积。則在表成和式的数$2^{k-1}PS$里，除掉$2^{k-1}P\frac{1}{2^k}$以外，所有的項都是整数。

b. 設k是适合条件$3^k\leqslant2n+1$的最大整数，而P是所有不大于$2n+1$而且与6互素的数的乘积。則在表成和式的数$3^{k-1}PS$里，除掉$3^{k-1}P\frac{1}{3^k}$以外，所有的項都是整数。

12. 当 $n\leqslant 8$ 时，定理可以直接核对。所以可以假定在 $n>8$ 时定理对于二項式 $a+b,(a+b)^2,\cdots,(a+b)^{n-1}$ 已經眞实了，来証明定理对于$(a+b)^n$ 也眞实。但是这个二項式展开以后的系数，除去兩头等于 1 以外，是下面的数:

$$\frac{n}{1},\quad \frac{n(n-1)}{1\cdot 2},\cdots,\frac{n(n-1)\cdots 2}{1\cdot 2\cdots(n-1)}.$$

这些数都是奇数的必要而且充分的条件是：它們的等于 n 的兩头是奇数，而且其余的数在把分母和分子里的奇数因子都去掉以后还是奇数。而假設 $n=2n_1+1$，这些数目可以表示成下列数列中的数:

$$\frac{n_1}{1},\quad \frac{n_1(n_1-1)}{1\cdot 2},\cdots,\frac{n_1(n_1-1)\cdots 2}{1\cdot 2\cdots(n-1)}.$$

由于 $n_1<n$，上面的数是奇数，在而且只在 n_1 有形式 2^k-1 时，也就是說 n 有形式 $2(2^k-1)+1=2^{k+1}-1$ 时。

第二章

1, a. 在曲綫 $y=f(x)$ 的有横坐标 x 的点的縱坐标上，有 $[f(x)]$ 个所說范圍的整点。

b. 設 T_1,T_2 和 T 分别表示下列范圍的整点的个数:

$$0<x<\frac{Q}{2},\quad 0<y<\frac{P}{Q}x;$$

$$0<y<\frac{P}{2},\quad 0<x<\frac{Q}{P}y;$$

$$0<x<\frac{Q}{2},\quad 0<y<\frac{P}{2}.$$

所求的等式可以从 $T_1+T_2=T$ 推出。

c. 設 T_1,T_2,T_3,T_4 分别表示下列范圍的整点的个数

$$x=0,\quad 0<y\leqslant r;$$

$$0<x\leqslant\frac{r}{\sqrt{2}},\quad 0<y\leqslant\sqrt{r^2-x^2};$$

$$0<y\leqslant\frac{r}{\sqrt{2}},\quad 0<x\leqslant\sqrt{r^2-y^2};$$

$$0<x\leqslant\frac{r}{\sqrt{2}},\quad 0<y\leqslant\frac{r}{\sqrt{2}}.$$

所求等式可以从 $T=1+4(T_1+T_2+T_3-T_4)$ 推出。

d. 設 T_1, T_2, T_3 分别表示下列范圍的整点的个数:

$$0<x\leqslant\sqrt{n},\quad 0<y\leqslant\frac{n}{x};$$

$$0<y\leqslant\sqrt{n},\quad 0<x\leqslant\frac{n}{y};$$

$$0<x\leqslant\sqrt{n},\quad 0<y\leqslant\sqrt{n}.$$

所求等式可以从 $T=T_1+T_2-T_3$ 推出。

2. 不超过 n 的正整数的个数等于 $[n]$。它們每一个都可以唯一地表示成形式 xk^m, 这里 k 是正整数; 而与一个已知的 x 对应的共有 $\left[\sqrt[m]{\frac{n}{x}}\right]$ 个这样形式的数。

3. 我們先証明所說条件的必要性。設 N 是整数, $N>1$。有条件 $[\alpha x]\leqslant N$ 的 x 值的个数可以表示成 $\frac{N}{\alpha}+\lambda$; $0\leqslant\lambda\leqslant C$, 而有条件 $[\beta y]\leqslant N$ 的 y 值的个数則可以表示成 $\frac{N}{\beta}+\lambda_1$; $0\leqslant\lambda_1\leqslant C_1$, 这里 C 和 C_1 都不依賴于 N。从 $\frac{N}{\alpha}+\lambda+\frac{N}{\beta}+\lambda_1=N$, 用 N 去除而且过渡到極限, 当 $N\to\infty$ 时, 我們得到 $\frac{1}{\alpha}+\frac{1}{\beta}=1$。最后这个等式对于有理数 $\alpha=\frac{a}{b}\,(a>b>0)$ 將会給出 $[\alpha b]=[\beta(a-b)]$。

假如所說条件有了。設 c 是整数, $c>0$, $x_0=\frac{c}{\alpha}+\xi$ 和 $y_0=\frac{c}{\beta}+\eta$ 是有条件 $x_0\geqslant\frac{c}{\alpha}$, $y_0\geqslant\frac{c}{\beta}$ 的最小整数。很明显地, $[\alpha x]\leqq c$ 对于 $x\leqq x_0$, 而 $[\beta y]\leqq c$ 对于 $y\leqq y_0$, $0<\xi<1$, $0<\eta<1$, $\alpha\xi$ 和 $\beta\eta$

都是無理数。由于 $x_0+y_0=c+\eta+\xi$，我們有 $\xi+\eta=1$, $\frac{\alpha\xi}{\alpha}+\frac{\beta\eta}{\beta}=1$；所以 $\alpha\xi$ 和 $\beta\eta$ 有一个而且只有一个小于 1，因此数 $[\alpha x_0]$ 和 $[\beta y_0]$ 有一个而且只有一个等于 c。

4, a. 所說的差数等于

$$\{\alpha x_1\},\ \{\alpha(x_2-x_1)\},\ \cdots,\ \{\alpha(x_t-x_{t-1})\},\ \{1-\alpha x_t\}.$$

它們全是非負的，它們的总和等于 1，而且它們的个数等于 $t+1$；所以其中至少有一个差数不超过 $\frac{1}{t+1}<\frac{1}{\tau}$，这样一来，就有一个小于 $\frac{1}{\tau}$ 而且有形式 $\{\pm\alpha Q\}$，$0<Q\leqslant\tau$ 的数目存在。从 $\pm\alpha Q==[\pm\alpha Q]+\{\pm\alpha Q\}$，假設 $\pm[\pm\alpha Q]=P$，我們得出 $|\alpha Q-P|<\frac{1}{\tau}$，$\left|\alpha-\frac{P}{Q}\right|<\frac{1}{Q\tau}$。

b. 假設 $X_0=[X]$, $Y_0=[Y]$, $\cdots$, $Z_0=[Z]$，讓 x, y, $\cdots$, z 通过值

$$x=0,1,\cdots,X_0;\ y=0,1,\cdots,Y_0;\ \cdots;\ z=0,1,\cdots,Z_0,$$

来討論由形式 $\{\alpha x+\beta y+\cdots+\gamma z\}$ 的数和 1 按不減小的次序所排成的数列。我們得到 $(X_0+1)(Y_0+1)\cdots(Z_0+1)+1$ 个数，从这些数我們得出 $(X_0+1)(Y_0+1)\cdots(Z_0+1)$ 个差数。其中至少有一个差数不大于

$$\frac{1}{(X_0+1)(Y_0+1)\cdots(Z_0+1)}<\frac{1}{XY\cdots Z}.$$

由此很容易可以得到所說的定理。

5. 我們有 $\alpha=cq+r+\{\alpha\}$; $0\leqslant r<c$,

$$\left[\frac{[\alpha]}{c}\right]=\left[q+\frac{r}{c}\right]=q,\ \left[\frac{\alpha}{c}\right]=\left[q+\frac{r+\{\alpha\}}{c}\right]=q.$$

6, a. 我們有

$$[\alpha+\beta+\cdots+\lambda]=[\alpha]+[\beta]+\cdots+[\lambda]+[\{\alpha\}+\{\beta\}+\cdots+\{\lambda\}],$$

b. 在 $n!$, $a!$, $\cdots$, $l!$ 里出現的素数 p 的方次数是

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots,\ \left[\frac{a}{p}\right]+\left[\frac{a}{p^2}\right]+\cdots,\ \cdots,\left[\frac{l}{p}\right]+\left[\frac{l}{p^2}\right]+\cdots.$$

因此
$$\left[\frac{n}{p^s}\right]\geqslant\left[\frac{a}{p^s}\right]+\cdots+\left[\frac{l}{p^s}\right].$$

7. 假定具有所說性質的数 a 存在着。把它表示成

$$a=q_kp^{k+1}+q_{k-1}p^k+\cdots+q_1p^2+q_0p+q';$$

$$0<q_k<p,\ 0\leqslant q_{k-1}<p,\ \cdots,\ 0\leqslant q_1<p,\ 0\leqslant q_0<p,\ 0\leqslant q'<p.$$

根据 § 1, b, 应該有

$$h=q_ku_k+q_{k-1}u_{k-1}+\cdots+q_1u_1+q_0u_0.$$

再有，对于任意的 $s=1, 2, \cdots, m$, 我們有

$$q_{s-1}u_{s-1}+q_{s-2}u_{s-2}+\cdots+q_1u_1+q_0u_0<u_s.$$

所以上面关于 h 的表示式应該完全和問題里所說的相合。

8, a. 設 x_1 是整数，$Q\leqslant\alpha<\beta\leqslant R,\ x_1<\alpha<\beta<x_1+1$。用分部积分法，我們得出

$$-\int_\alpha^\beta f(x)dx=\int_\alpha^\beta\rho'(x)f(x)dx=\rho(\beta)f(\beta)-\rho(\alpha)f(\alpha)-$$
$$-\sigma(\beta)f'(\beta)+\sigma(\alpha)f'(\alpha)+\int_\alpha^\beta\sigma(x)f''(x)dx.$$

特別地，当 $Q\leqslant x_1,\ x_1+1\leqslant R$, 过渡到極限，我們有

$$-\int_{x_1}^{x_1+1}f(x)dx=-\frac{1}{2}f(x_1+1)-\frac{1}{2}f(x_1)+\int_{x_1}^{x_1+1}\sigma(x)f''(x)dx.$$

所說的公式現在可以不費力地得出了。

b. 把問題 a 里的公式改写成:

$$\sum_{Q<x\leqslant R}f(x)=\int^R f(x)dx-\int^Q f(x)dx+\rho(R)f(R)-\rho(Q)f(Q)-$$

$$-\sigma(R)f'(R)+\sigma(Q)f'(Q)+\int_Q^{\infty}\sigma(x)f''(x)dx-\int_R^{\infty}\sigma(x)f''(x)dx.$$

就可以肯定所說公式的正确性。

c. 应用問題 b 的結果，我們得出

$$\ln 1+\ln 2+\cdots+\ln n=C+n\ln n-n+\frac{1}{2}\ln n+\int_n^{\infty}\frac{\sigma(x)}{x^2}dx=$$

$$=n\ln n-n+0(\ln n).$$

9, a, α) 我們有(§1, b)

$$\ln([n]!)=\sum_{p\leqslant n}\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots\right)\ln p. \qquad (1)$$

这里右边表示函数 $\ln p$ 的和式，对适合条件：p 是素数，$p>0$, $s>0$, $0<u\leqslant\frac{n}{p^s}$ 的整点 (p, s, u) 展开。这个和式中，与给定的 s 和 u 对应的部分，等于 $\Theta\left(\sqrt[s]{\frac{n}{u}}\right)$; 而与給定的 u 对应的部分，則等于 $\psi\left(\frac{n}{u}\right)$。

β) 对于 $n\geqslant 2$, 应用問題 α 的結果，我們有

$$\ln([n]!)-2\ln\left(\left[\frac{n}{2}\right]!\right)=\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-$$

$$-\psi\left(\frac{n}{4}\right)+\cdots\geqslant\psi(n)-\psi\left(\frac{n}{2}\right).$$

假設 $\left[\frac{n}{2}\right]=m$, 我們由此得出 ($[n]=2m$ 或者 $[n]=2m+1$):

$$\psi(n)-\psi\left(\frac{n}{2}\right)\leqslant\ln\frac{(2m+1)!}{(m!)^2}\leqslant$$

$$\leqslant\ln\left(2^m\frac{3\cdot5\cdots(2m+1)}{1\cdot2\cdots m}\right)\leqslant\ln(2^m3^m)<n,$$

$$\psi(n)=\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{2}\right)-\psi\left(\frac{n}{4}\right)+\psi\left(\frac{n}{4}\right)-$$
$$-\psi\left(\frac{n}{8}\right)+\cdots<n+\frac{n}{2}+\frac{n}{4}+\cdots=2n.$$

γ）我們有（問題β的解答和問題8，c的結果）

$$\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\cdots=\ln\frac{[n]!}{\left(\left[\frac{n}{2}\right]!\right)^2}=$$
$$=[n]\ln[n]-[n]-2\left[\frac{n}{2}\right]\ln\left[\frac{n}{2}\right]+2\left[\frac{n}{2}\right]+$$
$$+O(\ln n)=n\ln 2+O(\ln n).$$

再有，对于$s\geqslant 2$，我們得出（問題β）：

$$\Theta\left(\sqrt[s]{n}\right)-\Theta\left(\sqrt[s]{\frac{n}{2}}\right)+\Theta\left(\sqrt[s]{\frac{n}{3}}\right)-\cdots\begin{cases}<2\sqrt{n} & \text{所有情形}\\ =0 & \text{对于 } s>\tau;\ \tau=\left[\dfrac{\ln n}{\ln 2}\right].\end{cases}$$

所以

$$0\leqslant\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\cdots-$$
$$-\left(\Theta(n)-\Theta\left(\frac{n}{2}\right)+\Theta\left(\frac{n}{3}\right)-\Theta\left(\frac{n}{4}\right)+\cdots\right)<$$
$$<2\sqrt{n}+2\sqrt[3]{n}+2\sqrt[4]{n}+\cdots+2\sqrt[\tau]{n}<2(\sqrt{n}+\tau\sqrt[3]{n})=0(\sqrt{n}).$$

b. 从等式(1)，問題a，β的不等式和問題8，c的等式推出。

c. 問題b的等式对于充分大的m給出

$$\sum_{m<p\leqslant m^2}\frac{\ln p}{p}=\ln m+O(1)\geqslant\frac{\ln m}{2},\quad \sum_{m<p\leqslant m^2}\frac{4}{p}>1.$$

如果对于所有适合条件$m<p_n<p_{n+1}\leqslant m^2$的数偶$p_n$, p_{n+1}，不等式$p_{n+1}>p_n(1+\varepsilon)$成立，則就有

$$\sum_{r=0}^{\infty}\frac{4}{m(1+\varepsilon)^r}>1,$$

这对于充分大的m不可能成立。

d. 明显地，只要討論n是整数的情形就够了。

假設$\gamma(r)=\frac{\ln r}{r}$当$r$是素数，$\gamma(r)=0$当$r=1$或者$r$是复合数，我們就有(問題b)

$$\gamma(1)+\gamma(2)+\cdots+\gamma(r)=\ln r+\alpha(r);\ |\alpha(r)|<C_1,$$

这里C_1是常数。由此，对于$r>1$(我們認为$\alpha(1)=1$)

$$\gamma(r)=\ln r-\ln(r-1)+\alpha(r)-\alpha(r-1),$$

$$\sum_{0<p\leqslant n}\frac{1}{p}=T_1+T_2;\ \ T_1=\sum_{1<r\leqslant n}\frac{\ln r-\ln(r-1)}{\ln r},$$

$$T_2=\sum_{1<r\leqslant n}\frac{\alpha(r)-\alpha(r-1)}{\ln r}.$$

我們有(問題8, b)

$$T_1=\sum_{1<r\leqslant n}\frac{1}{r\ \ln r}+\sum_{1<r\leqslant n}\left(\frac{1}{2r^2\ln r}+\frac{1}{3r^3\ln r}+\cdots\right)=$$

$$=C_2+\ln\ln n+O\left(\frac{1}{\ln n}\right),$$

这里C_2是常数。再有我們得出

$$T_2=\alpha(2)\left(\frac{1}{\ln 2}-\frac{1}{\ln 3}\right)+\cdots+\alpha(n-1)\left(\frac{1}{\ln(n-1)}-\frac{1}{\ln n}\right)+\frac{\alpha(n)}{\ln n}$$

但是对于整数$m>1$，我們有

$$C_1\left(\frac{1}{\ln m}-\frac{1}{\ln(m+1)}\right)+C_1\left(\frac{1}{\ln(m+1)}-\frac{1}{\ln(m+2)}\right)+\cdots=\frac{C_1}{\ln m}.$$

所以級数

$$\alpha(2)\left(\frac{1}{\ln 2}-\frac{1}{\ln 3}\right)+\alpha(3)\left(\frac{1}{\ln 3}-\frac{1}{\ln 4}\right)+\cdots$$

是收斂的；因此如果C_3是它們的总和，則

$$T_2=C_3+O\left(\frac{1}{\ln n}\right).$$

e. 我們有

$$\ln\prod\left(1-\frac{1}{p}\right)=-\sum_{p\leqslant n}\frac{1}{p}-\sum_{p\leqslant n}\left(\frac{1}{2p^2}+\frac{1}{2p^3}+\cdots\right)=$$

$$=C'-\ln\ln n+O\left(\frac{1}{\ln n}\right),$$

这里 C' 是常数。由此，假設 $C'=\ln C_0$，我們得出所說的等式。

10, a. 从 § 2, c 推出。

b. 由于 $\theta(1)=\psi(1)=1$，函数 $\theta(a)$ 适合 § 2, a 的条件 1。設 $a=a_1a_2$ 是把 a 分成两个互素的因子的一个分解式。我們有

$$\sum_{d_1\diagdown a_1}\sum_{d_2\diagdown a_2}\theta(d_1d_2)=\psi(a)=\psi(a_1)\psi(a_2)=\sum_{d_1\diagdown a_1}\sum_{d_2\diagdown a_2}\theta(d_1)\theta(d_2). \tag{1}$$

如果 § 2, a 的条件 2 对于所有小于 a 的乘积成立了，則对于 $d_1d_2<a$ 我們有 $\theta(d_1d_2)=\theta(d_1)\theta(d_2)$，而等式 (1) 就給出 $\theta(a_1a_2)=\theta(a_1)\theta(a_2)$，这就是說，§ 2, a 的条件 2 对于所有等于 a 的乘积 a_1a_2 也成立。但是 § 2, a 的条件 2 对于等于 1 的乘积 1·1 成立。因此，它对于所有的乘积成立。

11, a. 設 $m>1$；对于除尽 a 的每个給定的 x_m，不定方程 $x_1\cdots x_{m-1}x_m=a$ 有 $\tau_{m-1}\left(\frac{a}{x_m}\right)$ 个解答。所以

$$\tau_m(a)=\sum_{x_m\diagdown a}\tau_{m-1}\left(\frac{a}{x_m}\right),$$

但是当 x_m 通过 a 的所有約数时，$d=\frac{a}{x_m}$ 以相反的順序通过这些約数。因此，

$$\tau_m(a)=\sum_{d\diagdown a}\tau_{m-1}(d).$$

所以如果定理对于函数 $\tau_{m-1}(a)$ 真实了，則它对于函数 $\tau_m(a)$ 也

眞实（問題10, a)。但是定理对于函数 $\tau_1(a)=1$ 眞实。这說明它总是眞实的。

b. 如果 $m>1$ 而且定理对于函数 $\tau_{m-1}(a)$ 眞实了，則我們就有

$$\tau_m(a)=\tau_m(p_1)\cdots\tau_m(p_k)=(\tau_{m-1}(1)+\tau_{m-1}(p_1))\cdots$$
$$\cdots(\tau_{m-1}(1)+\tau_{m-1}(p_k))=(1+m-1)^k=m^k.$$

但是定理对于函数 $\tau_1(a)$ 眞实。这就說明它总是眞实的。

c. 設 $\varepsilon=m\varepsilon_2$, $\varepsilon_2=2\eta$, $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 a 的标准分解式，并且 $p_1,\cdots,p_k$ 按照增加的順序排列。对于函数 $\tau_2(a)=\tau(a)$, 我們有

$$\frac{\tau(a)}{a^\eta}\leqslant\frac{\alpha_1+1}{2^{\alpha_1\eta}}\frac{\alpha_2+1}{3^{\alpha_2\eta}}\cdots\frac{\alpha_k+1}{(k+1)^{\alpha_k\eta}}.$$

在右边的乘积里每个因子都小于 $\frac{1}{\eta}$；而有条件 $r>2^{\frac{1}{\eta}}$ 的因子 $\frac{\alpha_{r-1}+1}{r^{\alpha_{r-1}\eta}}$ 則小于 $\frac{\alpha_{r-1}+1}{2^{\alpha_{r-1}}}\leqslant1$。所以，假設 $C=\left(\frac{1}{\eta}\right)^{2^{\frac{1}{\eta}}}$，我們得出

$$\frac{\tau(a)}{a^\eta}<C,\quad \lim_{a\to\infty}\frac{\tau(a)}{a^{\varepsilon_2}}\leqslant\lim_{a\to\infty}\frac{C}{a^\eta}=0.$$

对于 $m>2$, 很明显地，我們有 $\tau_m(a)\leqslant(\tau(a))^m$。所以

$$\lim_{a\to\infty}\frac{\tau_m(a)}{a^\varepsilon}\leqslant\lim_{a\to\infty}\left(\frac{\tau(a)}{a^{\varepsilon_2}}\right)^m=0.$$

d. 适合所說不等式的組 $x_1,\cdots,x_m$ 可以分成有号碼 $1,2,\cdots,[n]$ 的 $[n]$ 个集合。把有条件 $x_1\cdots x_m=a$ 的組放在有号碼 a 的集合里；这些組的个数正好是 $\tau_m(a)$。

12. 对于 $R(s)>1$, 表示 $\zeta(s)$ 的級数是絕对收斂的。所以

$$(\zeta(s)^m)=\sum_{n_1=1}^{\infty}\cdots\sum_{n_m=1}^{\infty}\frac{1}{(n_1\cdots n_m)^s},$$

并且对于已知正数 n，有条件 $n_1\cdots n_m=n$ 的組 $n_1,\cdots,n_m$ 的个数等于 $\tau_m(n)$。

13, a. 对于 $R(s)>1$，乘积 $P=\prod_p \frac{1}{1-\frac{1}{p^s}}$ 絕对收斂。由于 $\frac{1}{1-\frac{1}{p^s}}=1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots$，对于 $N>2$，我們有

$$\prod_{p\leqslant N}\frac{1}{1-\frac{1}{p^s}}=\sum_{0<n\leqslant N}\frac{1}{n^s}+\sum{}'\frac{1}{n^s},$$

这里在右边的第二个和式中，n 只通过大于N而又不被超过N的素数所除尽的数目。在 $N\to\infty$ 的極限情形，等式左边趋近 P，而右边的第一和式趋近 $\zeta(s)$，第二和式趋近零。

b. 設 $N>2$。假定除掉 $p_1,\cdots,p_k$ 以外沒有别的素数，我們得出(参看問題 a 的解答)

$$\prod_{j=1}^{k}\frac{1}{1-\frac{1}{p_j}}\geqslant\sum_{0<n\leqslant N}\frac{1}{n}.$$

这个不等式由于調和級数 $1+\frac{1}{2}+\frac{1}{3}+\cdots$ 的發散性，对于充分大的 N 不可能成立。

c. 假定除掉 $p_1,\cdots,p_k$ 以外沒有别的素数，我們得出(問題a)

$$\prod_{j=1}^{k}\frac{1}{1-\frac{1}{p_j^2}}=\zeta(2).$$

这个等式由于 $\zeta(2)=\frac{\pi^2}{6}$ 的無理性不可能成立。

14. 对于 $R(s)>1$，問題13, a 里关于 $\zeta(s)$ 的無穷乘积是絕对收斂的。所以

$$\ln\zeta(s)=\sum_{p}\left(\frac{1}{p^s}+\frac{1}{2p^{2s}}+\frac{1}{3p^{3s}}+\cdots\right),$$

这里 p 通过所有的素数。微分以后，我們有

$$\frac{\zeta'(s)}{\zeta(s)}=\sum_{p}\left(-\frac{\ln p}{p^s}-\frac{\ln p}{p^{2s}}-\frac{\ln p}{p^{3s}}-\cdots\right)=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

15. 設 $N>2$。应用§3, b 的定理，我們有

$$\prod_{p\leqslant N}\left(1-\frac{1}{p^s}\right)=\sum_{0<n\leqslant N}\frac{\mu(n)}{n^s}+\sum{}'\frac{\mu(n)}{n^s},$$

这里右边的第二个和式里 n 只通过大于 N 而且不被超过 N 的素数所除尽的整数。在極限情形，当 $N\to\infty$ 时，我們就得到所說的恒等式。

16, a. 应用§3, d 到下列情形

$$\delta=1,2,\cdots,[n],\quad f=1,1,\cdots,1.$$

于是很明显地 $S'=1$。再有 S_d 变成 δ 取倍于 d 的值的个数，即变成 $\left[\frac{n}{d}\right]$。

b, α) 問題 a 里等式的右边表示函数 $\mu(d)$ 的値的总和，它对范圍 $d>0$, $0<u\leqslant\frac{n}{d}$ 里的整点 (d,u) 展开。这个和式中，与給定的 u 对应的部分等于 $M\left(\frac{n}{u}\right)$。

β) 所說等式从下面的兩个等式逐項相减得到：

$$M(n)+M\left(\frac{n}{2}\right)+M\left(\frac{n}{3}\right)+M\left(\frac{n}{4}\right)+\cdots=1,$$

$$2M\left(\frac{n}{2}\right)+2M\left(\frac{n}{4}\right)+\cdots=2.$$

c. 設 $n_1=[n]$; $\delta_1,\delta_2,\cdots\delta_n$ 由后面的条件决定：δ_s 是 l 次乘方除尽 s 的最大整数，$f_s=1$。于是 $S'=T_{l,n}$, S_d 等于不超过 n 的

d^l 的倍数的个数，这就是說 $S_d=\left[\frac{n}{d^l}\right]$。由此就得到 $T_{l,n}$ 的所說表示式。

特别地，由于 $\zeta(2)=\frac{\pi^2}{6}$，对于不超过 n 而且不被大于 1 的平方数除尽的数目的个数 $T_{2,n}$，我們有

$$T_{2,n}=\frac{6}{\pi^2}n+O(\sqrt{n}).$$

17, a. 所說等式从 § 3, d 推出，如果我們讓

$$\delta_s=(x_s, a),\ f_s=f(x_s).$$

b. 所說等式从 § 3, d 推出，如果我們讓

$$\delta_s=(x_1^{(s)}, \cdots, x_k^{(s)}),\ f_s=f(x_1^{(s)}, \cdots, x_k^{(s)}).$$

c. 应用 § 3, d 到下列情形

$$\delta=\delta_1, \delta_2, \cdots, \delta_\tau,\ f=F\left(\frac{a}{\delta_1}\right), F\left(\frac{a}{\delta_2}\right), \cdots, F\left(\frac{a}{\delta_\tau}\right),$$

这里的那些 δ 表示 a 的所有約数，我們有

$$S'=F(a), S_d=\sum_{D\diagdown\frac{a}{d}} F\left(\frac{a}{dD}\right)=G\left(\frac{a}{d}\right).$$

d. 所說等式可以从下式推出

$$P'=f_1^{\sum\limits_{d\diagdown\delta_1}\mu(d)}f_2^{\sum\limits_{d\diagdown\delta_2}\mu(d)}\cdots f_n^{\sum\limits_{d\diagdown\delta_n}\mu(d)}.$$

18, a. 应用問題 17, a 的定理，讓 x 通过数目 $1, 2, \cdots, a$，而且取 $f(x)=x^m$。于是

$$S'=\psi_m(a), S_d=d^m+2^m d^m+\cdots+\left(\frac{a}{d}\right)^m d^m=d^m\sigma_m\left(\frac{a}{d}\right).$$

b. 我們有

$$\psi_1(a)=\sum_{d\diagdown a}\mu(d)\left(\frac{a^2}{2d}+\frac{a}{2}\right)=\frac{a}{2}\varphi(a).$$

同样的結果我們还可以更容易地得到。把数列 $1, 2, \cdots, a$ 里与 a 互素的数，先按增加的順序再按減少的順序写下来。这兩个数列中与首項等距离的对应項之和都等于 a；而每个数列的項数則等于 $\varphi(a)$。

c. 我們有

$$\psi_2(a)=\sum_{d\setminus a}\mu(d)\left(\frac{a^3}{3d}+\frac{a^2}{2}+\frac{a}{6}d\right)=\frac{a^2}{3}\varphi(a)+\frac{a}{6}(1-p_1)\cdots(1-p_k).$$

19, a. 应用問題 17, a 的定理，讓 x 通过数 $1, 2, \cdots, [z]$ 而且取 $f(x)=1$。于是 $S'=T_z$, S_d 等于不超过 z 的 d 的倍数的个数，也就是說 $S_d=\left[\frac{z}{d}\right]$。

b. 我們有

$$T_z=\sum_{d\setminus a}\mu(d)\frac{z}{d}+O(\tau(a))=\frac{z}{a}\varphi(a)+O(a^{\varepsilon}).$$

c. 从問題 a 的等式推出。

20. 应用問題 17, a 的定理，讓 x 通过数 $1, 2, \cdots, N$，这里 $N>>a$，而且取 $f(x)=\frac{1}{x^s}$。于是我們得到

$$\sum_{x\leqslant N}{}'\frac{1}{x^s}=\sum_{d\setminus a}\mu(d)\sum_{0<x\leqslant\frac{N}{d}}\frac{1}{d^s x^s}=\sum_{d\setminus a}\frac{\mu(d)}{d^s}\sum_{0<x\leqslant\frac{N}{d}}\frac{1}{x^s}.$$

在極限情形，当 $N\to\infty$ 时，我們得到所說的恒等式。

21, a. 应用問題 17, b 的定理，討論在可能率 P_N 的定义里的組 $x_1, x_2, \cdots, x_k$，而且取 $f(x_1, x_2, \cdots, x_k)=1$。于是 $P_N=\frac{S'}{N^k}$, $S_d=\left[\frac{N}{d}\right]^k$，而且我們得到

$$P_N=\frac{\sum_{d=1}^{N}\mu(d)\left[\frac{N}{d}\right]^k}{N^k}=\sum_{d=1}^{N}\frac{\mu(d)}{d^k}+O\left(\sum_{d=1}^{N}\frac{1}{Nd^{k-1}}\right).$$

所以

$$P_N=(\zeta(k))^{-1}+O(\Delta);\quad \Delta=\frac{1}{N}\text{对于 } k>2,\ \Delta=\frac{\ln N}{N}\text{对于 } k=2。$$

b. 我們有 $\zeta(2)=\frac{\pi^2}{6}$。

22, a. 初等的論証說明，在范圍 $u^2+v^2\leqslant\rho^2$, $\rho>0$ 里的整点 (u, v) 的个数，不計算点 $(0, 0)$, 等于 $\pi\rho^2+O(\rho)$。应用問題 17, b 的定理，討論在范圍 $x^2+y^2\leqslant r^2$ 里不同于 $(0, 0)$ 的整点的坐标 x, y, 而且假設 $f(x,y)=1$。于是 $T=S'+1$, S_d 等于在范圍 $u^2+v^2\leqslant\left(\frac{r}{d}\right)^2$ 里不同于 $(0, 0)$ 的整点的个数。所以

$$S_d=\pi\frac{r^2}{d^2}+O\left(\frac{r}{d}\right),$$

$$T=\sum_{d=1}^{[r]}\mu(d)\pi\frac{r^2}{d^2}+O\left(\sum_{d=1}^{[r]}\frac{r}{d}\right)=\frac{6}{\pi}r^2+O(r\ln r).$$

b. 作与上面类似的論証，我們得到

$$T=\sum_{d=1}^{[r]}\mu(d)\frac{4}{3}\pi\frac{r^3}{d^3}+O\left(\sum_{d=1}^{[r]}\frac{r^2}{d^2}\right)=\frac{4\pi r^2}{3\zeta(3)}+O(r^2).$$

23, a. 数 $a=p_1^{a_1}\cdots p_k^{a_k}$ 的約数中，不被大于 1 的平方数除尽，而且有 κ 个素約数的約数 d 的个数等于 $\binom{k}{\kappa}$; 并且 $\mu(d)=(-1)^\kappa$。所以

$$\sum_{d\backslash a}\mu(d)=\sum_{\kappa=0}^{k}\binom{k}{\kappa}(-1)^\kappa=(1-1)^k=0.$$

b. 設 a 有問題 a 里同样的形式。只要討論 $m<k$ 的情形就够了。对于所說的和式，我們有两个表示式

$$\sum\mu(d)=\binom{k}{0}-\binom{k}{1}+\cdots+(-1)^m\binom{k}{m}=$$

$$=(-1)^m\left(\binom{k}{m+1}-\binom{k}{m+2}+\cdots\right).$$

如果 m 是偶数，則对于 $m\leqslant\frac{k}{2}$，第一个式子 >0，而对于 $m=\frac{k}{2}$，第二个式子 $\geqslant 0$。如果 m 是奇数，則对于 $m\leqslant\frac{k}{2}$，第一个式子 <0，而对于 $m>\frac{k}{2}$，第二个式子 $\leqslant 0$。

c. 証明与 §3, d 里差不多，但是要利用問題 b 的結果。

d. 証明与問題 17, a 和 b 里差不多。

24. 設 d 通过数 a 的所有約数，$\Omega(d)$ 是 d 的素約数的个数，$\Omega(a)=s$。按照問題里所作的說明，我們有(假設 N 充分大)

$$\pi(N,q,l)\leqslant\sum_{\Omega(d)\leqslant m}\mu(d)\left(\frac{N}{qd}+\theta_d\right)=T+T_0-T_1;\ |\theta_d|\leqslant 1,$$

$$|T|\leqslant\sum_{\Omega(d)\leqslant m}1,\quad T_0=\frac{N}{q}\sum_{d}\frac{\mu(d)}{d},\quad |T_1|=\sum_{\Omega(d)>m}\frac{N}{qd}.$$

再有我們得出

$$|T|\leqslant\sum_{n=0}^{m}\binom{s}{n}\leqslant s^m\leqslant e^{hm}<e^{5r^{1-\varepsilon}\ln r}\frac{qr}{N}\frac{N}{qr}=O(\Delta),$$

$$T_0=\frac{N}{q}\frac{\prod\limits_{p\leqslant e^h}\left(1-\frac{1}{p}\right)}{\prod\limits_{p\backslash q}\left(1-\frac{1}{p}\right)}=O(\Delta).$$

最后用 C_1 和 C_2 表示某些常数，我們有

$$|T_1|\leqslant\frac{N}{q}\sum_{n=m+1}^{s}\sum_{\Omega(d)=n}\frac{1}{d}\leqslant\frac{N}{q}\sum_{n=m+1}^{s}\frac{\left(\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p_s}\right)^n}{n!}\leqslant$$

$$\leqslant\frac{N}{q}\sum_{n=m+1}^{s}\left(\frac{C_1+\ln r}{4\ln r}e\right)^n\leqslant$$

$$\leqslant\frac{N}{q}\sum_{n=m+1}^{s}\left(\frac{3}{4}\right)^n<C_2\frac{N}{q}r^{-4\ln\frac{4}{3}}=O(\Delta).$$

25. 数目 a 的每一个有条件 $d_1<\sqrt{a}$ 的約数 d_1, 对应于另一个有条件 $d_2>\sqrt{a}$, $d_1d_2=a$ 的約数 d_2。并且 $\mu(d_1)=\mu(d_2)$。所以

$$2\sum_{d_1}\mu(d)=\sum_{d_1}\mu(d)+\sum_{d_2}\mu(d)=\sum_{d\diagdown a}\mu(d)=O.$$

26. 数 d 不被大于 1的平方数除尽，而且适合条件 $\varphi(d)=k$, 我們成对地討論这样的数，使得在每一对里出現奇数 d_1 和偶数 $2d_1$, 就有 $\mu(d_1)+\mu(2d_1)=O$。

27. 設 $p_1,\cdots,p_k$ 是不同的素数。假設 $a=p_1\cdots p_k$, 我們有

$$\varphi(a)=(p_1-1)\cdots(p_k-1),$$

然而当 $p_1,\cdots,p_k$ 以外沒有别的素数存在时，只有 1 与 a 互素，我們就有 $\varphi(a)=1$。

28, a. 在数 $s\delta: s=1,2,\cdots,\frac{a}{\delta}$ 中間找出所說的数。但是因为 $(s\delta,a)=\delta$ 在而且只在 $\left(s,\frac{a}{\delta}\right)=1$ 时 (第一章 § 2, e), 所以問題里所提出的断言是眞实的，而且我們有

$$a=\sum_{\delta\diagdown a}\varphi\left(\frac{a}{\delta}\right)=\sum_{d\diagdown a}\varphi(d).$$

b. α) 設 $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 a 的标准分解式，根据 9, 函数 $\varphi(a)$

是可乘的，并且

$$p_s^{\alpha_s}=\sum_{d\diagdown p_s^{\alpha_s}}\varphi(d),\ p_s^{\alpha_s-1}=\sum_{d\diagdown p_s^{\alpha_s-1}}\varphi(d),\ p_s^{\alpha_s}-p_s^{\alpha_s-1}=\varphi\left(p_s^{\alpha_s}\right).$$

β) 对于整数 $m>0$，我們有

$$m=\sum_{d\diagdown m}\varphi(d).$$

所以
$$\varphi(a)=\sum_{d\diagdown a}\mu(d)\frac{a}{d}.$$

29. 我們有（p 通过所有素数）

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\prod_p\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\cdots\right)=\prod_p\frac{1-\frac{1}{p^s}}{1-\frac{1}{p^{s-1}}}=\frac{\zeta(s-1)}{\zeta(s)}.$$

30. 我們有

$$\varphi(1)+\varphi(2)+\cdots+\varphi(n)=\sum_{d\diagdown 1}\frac{\mu(d)}{d}+2\sum_{d\diagdown 2}\frac{\mu(d)}{d}+\cdots+n\sum_{d\diagdown n}\frac{\mu(d)}{d}=$$

$$=\sum_{d=1}^{n}\mu(d)\left(1+2+\cdots+\left[\frac{n}{d}\right]\right)=\sum_{d=1}^{n}\mu(d)\frac{n^2}{2d^2}+O(n\ln n)=$$

$$=\frac{n^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(n\ln n)=\frac{3}{\pi^2}n^2+O(n\ln n).$$

第三章

1, a. 从

$$P=a_n10^{n-1}+a_{n-1}10^{n-2}+\cdots+a_1,$$

由于 $10\equiv1\pmod 9$，我們有

$$P \equiv a_n + a_{n-1} + \cdots + a_1 \pmod{9}.$$

因此，P 是 3 的倍数，在而且只在它的各位数字的和是 3 的倍数时；而它是 9 的倍数，在而且只在它的各位数字的和是 9 的倍数时。

再由于 $10 \equiv -1 \pmod{11}$，我們有

$$P \equiv (a_1 + a_3 + \cdots) - (a_2 + a_4 + \cdots) \pmod{11}.$$

因此 P 是 11 的倍数，在而且只在它的奇数位（从右面算起）数字的总和与它的偶数位数字的总和的差数是 11 的倍数时。

b. 从

$$P = b_n 100^{n-1} + b_{n-1} 100^{n-2} + \cdots + b_1,$$

由于 $100 \equiv -1 \pmod{101}$，我們有

$$P \equiv (b_1 + b_3 + \cdots) - (b_2 + b_4 + \cdots) \pmod{101}.$$

所以 P 是 101 的倍数，在而且只在 $(b_1 + b_3 + \cdots) - (b_2 + b_4 + \cdots)$ 是 101 的倍数时。

c. 从

$$P = c_n 1000^{n-1} + c_{n-1} 1000^{n-2} + \cdots + c_1,$$

由于 $1000 \equiv 1 \pmod{37}$，我們有

$$P \equiv c_n + c_{n-1} + \cdots + c_1 \pmod{37}.$$

所以 P 是 37 的倍数，在而且只在 $c_n + c_{n-1} + \cdots + c_1$ 是 37 的倍数时。由于 $1000 \equiv -1 \pmod{7 \cdot 11 \cdot 13}$，我們有

$$P \equiv (c_1 + c_3 + \cdots) - (c_2 + c_4 + \cdots) \pmod{7 \cdot 11 \cdot 13}。$$

所以 P 是 7, 11, 13 中一个的倍数，在而且只在 $(c_1 + c_3 + \cdots) - (c_2 + c_4 + \cdots)$ 是这个数的倍数时。

2, a, α) 当 x 通过模 m 的完全剩余組时，$ax + b$ 也通过这个完全剩余組；而数 $ax + b$ 的非負的最小剩余 r 則通过 $0, 1, \cdots, m-1$。所以

$$\sum_{x}\left\{\frac{ax+b}{m}\right\}=\sum_{r=0}^{m-1}\frac{r}{m}=\frac{1}{2}(m-1).$$

β) 应用第二章問題 18 b 的結果，我們得出

$$\sum_{\xi}\left\{\frac{a\xi}{m}\right\}=\frac{\psi_1(m)}{m}=\frac{1}{2}\varphi(m).$$

b. 在 $t=1$ 的情形，我們有

$$[f(N+m)]-[f(N)]=a,$$

$$\sum\delta=\sum_{x=N+1}^{N+m}[f(x)]-\frac{1}{2}[f(N+m)]+\frac{1}{2}[f(N)]-\frac{1}{2}+\frac{1}{2}m=$$

$$=\sum_{x=N+1}^{N+m}f(x)-\sum_{x=N+1}^{N+m}\{f(x)\}-\frac{1}{2}a+\frac{1}{2}(m-1)=S;$$

$t>1$ 的情形很容易可以化成这种情形。

c. 設 N, M, P_1, P_2 都是整数，$M>0, P_1>0, P_2>0$。有頂点 $(N,0), (N,P_1), (N+M,0), (N+M,P_2)$ 的梯形乃是問題 b 所討論的梯形的特別情形。所以等式(1)对于它成立。而对于这样的梯形，等式(1)还可以用更簡單的方法得到。我們只要討論等于这个梯形兩倍的長方形 $(N,0), (N,P_1+P_2), (N+M,0), (N+M, P_1+P_2)$。对于这个長方形，显然有与等式(1)类似的等式

$$\sum{}'\delta=S'.$$

由此根据 $\sum'\delta=2\sum\delta, S'=2S$，我們就得到等式(1)。

从这个結果，关于問題里所說的三角形的类似的公式很容易可以引出。然而写在下面的論証也有它的好处：所說的三角形可以从一个有整点作为頂点的平行四边形分成兩个相等的三角形而得到。設 S 是平行四边形的面积而且 $T=\sum\delta$，这个和式对平行

四边形的所有整点展开，并且 δ 的决定与問題 b 里一样。如果我們能够証明 $S=T$，也就証明了我們所关心的三角形的性質。我們来討論有無限伸長的边 A 的正方形。整个平面可以分成無穷多个有所說形式的平行四边形。設 k 是在正方形里面的平行四边形的个数，而 R 是正方形內整点的个数。当 $A\to\infty$ 时我們得出

$$\lim\frac{kS}{A^2}=1,\quad \lim\frac{A^2}{R}=1,\quad \lim\frac{R}{kT}=1.$$

这些等式逐項相乘，我們得到

$$\lim\frac{S}{T}=1,\quad S=T.$$

3, a. 設 r 是数 $ax+[c]$ 对于模 m 的非負的最小剩余，我們有

$$S=\sum_{r=0}^{m-1}\left\{\frac{r+\Phi(r)}{m}\right\},$$

这里 $\varepsilon\leqslant\Phi(r)\leqslant\varepsilon+h$; $\varepsilon=\{c\}$。对于 $m\leqslant 2h+1$，定理显然真实。所以我們只考虑 $m>2h+1$ 的情形。假設

$$\left\{\frac{r+\Phi(r)}{m}\right\}-\frac{r}{m}=\delta(r),$$

我們有 $-1+\frac{\varepsilon}{m}\leqslant\delta(r)\leqslant\frac{h+\varepsilon}{m}$ 对于 $r=m-[h+\varepsilon],\cdots,m-1$; $\frac{\varepsilon}{m}\leqslant\delta(r)\leqslant\frac{h+\varepsilon}{m}$ 在其他的情形。所以

$$-[h+\varepsilon]+\varepsilon\leqslant S-\frac{m-1}{2}\leqslant h+\varepsilon,\quad \left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

b. 我們有

$$S=\sum_{z=0}^{m-1}\left\{\frac{az+\psi(z)}{m}\right\};\ \psi(z)=m(AM+B)+\frac{\lambda}{m}z.$$

应用問題 a 的定理，讓 $h=|\lambda|$。于是我們就得到所說的結果。

c. 我們得出

$$S=\sum_{z=0}^{m-1}\left\{f(M)+\frac{az}{m}+\frac{\theta z}{m^2}+\frac{f''(M+z_0)}{2}z^2\right\},\quad 0<z_0<m-1.$$

应用問題 a 的定理，讓 $h=1+\frac{k}{2}$。我們就得到所說的結果。

4. 把 A 分割成連分式。設 $Q_n=Q'$ 是近似分数的不超过 m 的最大分母，我們有(第一章問題 4, b)

$$A=\frac{P'}{Q'}+\frac{\theta'}{Q'm},\ (P',Q')=1,\ |\theta'|<1.$$

这时由于 $m<Q_{n+1}\leqslant(q_{n+1}+1)Q_n\leqslant CQ_n$，这里 C 是不超过所有 q_s+1 的常数，对于有条件 $H'Q'\leqslant m$ 的最大整数 H'，可以推出 $H'<C$。应用問題 3, b 的定理，我們得出

$$\left|\sum_{x=M}^{M+H'Q'-1}\{Ax+B\}-\frac{1}{2}H'Q'\right|\leqslant\frac{3}{2}C.$$

設 $m_1=m-H'Q'$。如果 $m_1>0$，則用前面选取与 m 有关的数 Q' 和 H' 同样的方法来挑选与 m_1 有关的 Q'' 和 H''，我們得出

$$\left|\sum_{x=M_1}^{M_1+H''Q''-1}\{Ax+B\}-\frac{1}{2}H''Q''\right|\leqslant\frac{3}{2}C.$$

設 $m_2=m_1-H''Q''$。如果 $m_2>0$，則与前面一样，我們得出

$$\left|\sum_{x=M_2}^{M_2+H'''Q'''-1}\{Ax+B\}-\frac{1}{2}H'''Q'''\right|\leqslant\frac{3}{2}C.$$

这样繼續下去，直到有某个 $m_k=0$ 时才止。那时我們得到($H'Q'+$ $+H''Q''+\cdots+H^{(k)}Q^{(k)}=m$)

$$\left|\sum_{x=M}^{M+m-1}\{Ax+B\}-\frac{1}{2}m\right|<\frac{3}{2}Ck.$$

数 $Q',Q'',\cdots,Q^{(k)}$ 适合条件

$$m \geqslant Q' > m_1 \geqslant Q'' > m_2 \geqslant \cdots > m_{k-1} \geqslant Q^{(k)} \geqslant 1.$$

所以$k=0(\ln m)$（第一章問題3），因此問題里所說的公式成立。

5, a. 用S表示等式左边的和式。設$\tau = A^{\frac{1}{3}}$。对于$\tau \leqslant 40$定理显然真实。所以我們假設$\tau > 40$。取$M_1 = [Q+1]$，我們找出有条件

$$f'(M_1) = \frac{a_1}{m_1} + \frac{\theta_1}{m_1\tau}; \quad 0 < m_1 \leqslant \tau, \ (a_1, m_1) = 1, \quad |\theta_1| < 1$$

的数a_1, m_1, θ_1。取$M_2 = M_1 + m_1$，用同样的步驟找出a_2, m_2, θ_2；取$M_3 = M_2 + m_2$，找出a_3, m_3, θ_3；等等，直到$M_{s+1} = M_s + m_s$有条件$0 \leqslant [R] - M_{s+1} < [\tau]$时才止。应用問題3，c的定理，我們得出

$$\left| S - \frac{1}{2}\ (m_1 + m_2 + \cdots + m_s + [R] - M_{s+1})\ \right| <$$

$$< s\frac{k+3}{2} + \frac{1}{2}([R] - M_{s+1}),$$

$$\left| S - \frac{1}{2}(R - Q) \right| < s\frac{k+3}{2} + \frac{\tau+1}{2}.$$

間隔$\frac{a}{m} - \frac{1}{m\tau} \leqslant f'(x) \leqslant \frac{a}{m} + \frac{1}{m\tau}$的長度不超过$\frac{2A}{m\tau}$。因此在$m_1, m_2, \cdots, m_s$中与同一个分数$\frac{a}{m}$相关的数目的个数$\leqslant \frac{2A}{m^2\tau} + 1$。設$a_1$和$a_2$是与給定的$m$对应的$a$的最小值和最大值。我們有

$$\frac{a_2 - a_1}{m} - \frac{2}{m\tau} \leqslant \frac{k(R-Q)}{A}; \quad a_2 - a_1 + 1 \leqslant \frac{k(R-Q)m}{A} + 1.05.$$

因此，在$m_1, m_2, \cdots, m_k$中与已知的m相关的数目的个数

$$< \left(\frac{2A}{m^2\tau} + 1\right)\left(\frac{k(R-Q)m}{A} + 1.05\right) =$$

$$= \frac{k(R-Q)}{\tau}\left(\frac{2}{m} + \frac{m}{\tau^2}\right) + \left(\frac{2A}{m^2\tau} + 1\right)1.05.$$

最后这个式子对于所有$m = 1, 2, \cdots, [\tau]$求总和，我們得到

$$s<\frac{k(R-Q)}{\tau}\left(2\ln\ \ +2+\frac{\tau^2+\tau}{2\tau^2}\right)\frac{10A}{3\tau}1.05<$$

$$<\frac{k(R-Q)}{\tau}\ln A+\frac{7}{2}\frac{A}{\tau}.$$

$$\left|S-\frac{1}{2}(R-Q)\right|<2\frac{k^2(R-Q)}{\tau}\ln A+8k\frac{A}{\tau}.$$

b. 我們有

$$\left|\sum_{Q<x\leqslant R}\{f(x)+1-\sigma\}-\frac{1}{2}(R-Q)\right|<\Delta,$$

$$\left|\sum_{Q<x\leqslant R}\{f(x)\}-\frac{1}{2}(R-Q)\right|<\Delta,$$

于是，讓 $\delta(x)=\{f(x)+1-\sigma\}-\{f(x)\}$，我們得出

$$\left|\sum_{Q<x\leqslant R}\delta(x)\right|<2\Delta.$$

但是对于 $\{f(x)\}<\sigma$，我們有 $\delta(x)=1-\sigma$，而对于 $\{f(x)\}>\sigma$，我們有 $\delta(x)=-\sigma$。所以 $|(1-\sigma)\psi(\sigma)-\sigma(R-Q-\psi(\sigma))|<2\Delta$，于是我們就得到所說的公式。

6, a. 应用第二章問題1, c的公式。讓 $f(x)=\sqrt{r^2-x^2}$，在間隔 $0\leqslant x\leqslant\frac{r}{\sqrt{2}}$ 里，我們有

$$f'(x)=-\frac{x}{\sqrt{r^2-x^2}},\quad f''(x)=\frac{-r^2}{(r^2-x^2)^{3/2}},$$

$$\frac{1}{r}\leqslant|f''(x)|\leqslant\frac{\sqrt{8}}{r}.$$

所以（問題5, a和第二章問題8, a）

$$T=4r+8\int_0^{\frac{r}{\sqrt{2}}}\sqrt{r^2-x^2}dx+8\rho\left(\frac{r}{\sqrt{2}}\right)\frac{r}{\sqrt{2}}-$$

$$-8\rho(0)\cdot r-4\frac{r}{\sqrt{2}}-4\frac{r^2}{2}+8\frac{r}{\sqrt{2}}\left\{\frac{r}{\sqrt{2}}\right\}+$$

$$+O\left(r^{\frac{2}{3}}\ln r\right)=\pi r^2+O(r^{\frac{2}{3}}\ln r).$$

b. 我們有(第二章問題 11, d 和 1, d)

$$\tau(1)+\tau(2)+\cdots+\tau(n)=2\sum_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

只要考虑 $n>64$ 的情形就够了。設$X=2n^{\frac{1}{3}}$，把間隔 $X<x\leqslant\sqrt{n}$ 分成$O(\ln n)$个形式 $M<x\leqslant M'$, $M'\leqslant 2M$ 的間隔。讓$f(x)=\frac{n}{x}$, 在間隔 $M<x\leqslant M'$ 里，我們有

$$f'(x)=-\frac{n}{x^2},\ f''(x)=\frac{2n}{x^3},\quad \frac{n}{4M^3}\leqslant f''(x)\leqslant\frac{8n}{4M^3}.$$

所以(問題 5, a)

$$\sum_{M<x\leqslant M'}\left\{\frac{n}{x}\right\}=\frac{1}{2}(M'-M)+O(n^{\frac{1}{3}}\ln n),$$

$$\sum_{0<x\leqslant\sqrt{n}}\left\{\frac{n}{x}\right\}=\frac{1}{2}\sqrt{n}+O\left(n^{\frac{1}{3}}(\ln n)^2\right).$$

再有(第二章問題 8, b)

$$\sum_{0<x\leqslant\sqrt{n}}\frac{n}{x}=En+\frac{1}{2}n\ln n+\rho(\sqrt{n})\sqrt{n}+O(1).$$

所以

$$\tau(1)+\tau(2)+\cdots+\tau(n)=2En+n\ln n+2\rho(\sqrt{n})\sqrt{n}-$$

$$-\sqrt{n}-n+2\sqrt{n}\{\sqrt{n}\}+O\left(n^{\frac{1}{3}}(\ln n)^2\right)=$$

$$=n(\ln n+2E-1)+O(n^{\frac{1}{3}}(\ln n)^2).$$

7. 設組是不規則的，s 是使得組里有 2^s 項的数的个数是奇数的最大整数，S 是有 2^s 項的数的一个。在 S 里把 2^s 項去掉，而且适当地增加或者減少小于 2^s 并且在組里还是出現奇数次的各

項，就可以使这个組变成規則的。

設組是不規則的，把組里的一个数 T 換成一个小于 T 的数，T 里的各項至少有一个不再在这个数里出現。这样一来，这个組就变成不規則的了。

8, a. 把数 $H=3^n+3^{n-1}+\cdots+3+1$ 加在用所說方法表示的数上以后，我們得到的数，相当于在原来的表示式中讓 $x_n, x_{n-1}, \cdots$ $\cdots, x_1, x_0$ 通过 0, 1, 2 时所得的数，也就是說我們得到的所有数是 $0, 1, \cdots, 2H$。

b. 用所說的方法我們得到 $m_1m_2\cdots m_k$ 个数，它們对于模 $m_1m_2\cdots m_k$ 都不同余，因为从

$$x_1+m_1x_2+m_1m_2x_3+\cdots+m_1m_2\cdots m_{k-1}x_k\equiv$$
$$\equiv x_1'+m_1x_2'+m_1m_2x_3'+\cdots+m_1m_2\cdots m_{k-1}x_k' \pmod{m_1m_2\cdots m_k},$$

我們順次得出

$$x_1\equiv x_1' \pmod{m_1},\quad x_1=x_1';\quad m_1x_2\equiv m_1x_2' \pmod{m_1m_2},$$
$$x_2=x_2';\quad m_1m_2x_3\equiv m_1m_2x_3' \pmod{m_1m_2m_3},\quad x_3=x_3',$$

等等。

9, a. 用所說的方法我們得到 $m_1m_2\cdots m_k$ 个数，它們对于模 $m_1m_2\cdots m_k$ 都不同余，因为从

$$M_1x_1+M_2x_2+\cdots+M_kx_k\equiv$$
$$\equiv M_1x_1'+M_2x_2'+\cdots+M_kx_k' \pmod{m_1m_2\cdots m_k}$$

推出（与 M_s 不同的每一个 M_j，都是 m_s 的倍数）

$$M_sx_s\equiv M_sx_s' \pmod{m_s},\quad x_s\equiv x_s' \pmod{m_s},\quad x_s=x_s'.$$

b. 用所說的方法我們得到 $\varphi(m_1)\varphi(m_2)\cdots\varphi(m_k)=\varphi(m_1m_2\cdots$ $\cdots m_k)$ 个数，根据問題 a 的定理，它們对于模 $m_1m_2\cdots m_k$ 都不同余，而且由于 $(M_1x_1+M_2x_2+\cdots+M_kx_k, m_s)=(M_sx_s, m_s)=1$，它們都与 $m_1m_2\cdots m_k$ 互素。

c. 根据問題 a 的定理，当 $x_1, x_2, \cdots, x_k$ 通过模 $m_1m_2\cdots m_k$ 的

完全剩余組时，数 $M_1x_1+M_2x_2+\cdots+M_kx_k$ 通过模 $m_1m_2\cdots m_k$ 的完全剩余組。这样的数与 $m_1m_2\cdots m_k$ 互素，在而且只在 $(x_1,m_1)=$ $=(x_2,m_2)=\cdots=(x_k,m_k)=1$ 时。所以 $\varphi(m_1m_2\cdots m_k)=\varphi(m_1)\varphi(m_2)\cdots$ $\cdots\varphi(m_k)$。

d. 要从数列 $1, 2, \cdots, p^\alpha$ 得到所有与 p^α 互素的数目，只要在这个数列里划掉所有 p 的倍数，也就是 $p, 2p, \cdots p^{\alpha-1}p$。所以 $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$。由此再利用第二章 § 4, c 的定理，关于 $\varphi(a)$ 的表示式立刻可以推出：

10, a. 第一个断言从下面的式子推出：

$$\left\{\frac{x_1}{m_1}+\cdots+\frac{x_k}{m_k}\right\}=\left\{\frac{M_1x_1+\cdots+M_kx_k}{m}\right\};$$

第二个断言从下面的式子推出：

$$\left\{\frac{\xi_1}{m_1}+\cdots+\frac{\xi_k}{m_k}\right\}=\left\{\frac{M_1\xi_1+\cdots+M_k\xi_k}{m}\right\}.$$

b. 分数 $\left\{\frac{f_1(x_1,\cdots,w_1)}{m_1}+\cdots+\frac{f_k(x_k,\cdots,w_k)}{m_k}\right\}$ 等于分数

$$\left\{\frac{f_1(M_1x_1+\cdots+M_kx_k,\cdots,M_1w_1+\cdots+M_kw_k)}{m_1}+\cdots+\right.$$
$$\left.+\frac{f_k(M_1x_1+\cdots+M_kx_k,\cdots,M_1w_1+\cdots+M_kw_k)}{m_k}\right\}$$

也就是等于分数 $\left\{\frac{f_1(x,\cdots,w)}{m_1}+\cdots+\frac{f_k(x,\cdots,w)}{m_k}\right\}$。由此显然可以得到第一个断言。第二个断言可以用类似的方法証明。

11, a. 当 a 是 m 的倍数时，我們有

$$\sum_x e^{2\pi i\frac{ax}{m}}=\sum_x 1=m.$$

当 a 不被 m 除尽时，我們有

$$\sum_{x} e^{2\pi i\frac{ax}{m}}=\frac{e^{2\pi i\frac{am}{m}}-1}{e^{2\pi i\frac{a}{m}}-1}=0.$$

b. 当 α 不是整数时，左边等于

$$\left|\frac{e^{2\pi i\alpha(M+P)}-e^{2\pi i\alpha M}}{e^{2\pi i\alpha}-1}\right|\leqslant\frac{1}{\sin\pi(\alpha)}\leqslant\frac{1}{h(\alpha)}.$$

c. 根据問題 b 的定理，左边不超过 T_m，这里

$$T_m=\sum_{a=1}^{m-1}\frac{1}{h\left(\frac{a}{m}\right)}.$$

但是对于奇数 m

$$T_m<m\sum_{0<a<\frac{m}{2}}\ln\frac{2a+1}{2a-1}=m\ln m,$$

而对于偶数 m

$$T_m<\frac{m}{2}\sum_{0<a\leqslant\frac{m}{2}}\ln\frac{2a+1}{2a-1}+\frac{m}{2}\sum_{0<a<\frac{m}{2}}\ln\frac{2a+1}{2a-1}<m\ln m.$$

对于 $m\geqslant 6$，由于 $\frac{1}{2}-\frac{1}{3}=\frac{1}{6}$，界限 $m\ln m$ 可以减小

$$2\frac{m}{6}\sum_{0<a\leqslant\frac{m}{6}}\ln\frac{2a+1}{2a-1}=\frac{m}{3}\ln\left(2\left[\frac{m}{6}\right]+1\right).$$

这最后的式子当 $m\geqslant 12$ 时 $>\frac{m}{2}$，而且当 $m\geqslant 60$ 时它 $>m$。

12, a. 設 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解式。讓 $p_1^{\alpha_1}=m_1,\cdots$ $\cdots,p_k^{\alpha_k}=m_k$，用問題 10, a 的符号，我們有

$$\sum_{\xi_1} e^{2\pi i\frac{\xi_1}{m_1}}\cdots\sum_{\xi_k} e^{2\pi i\frac{\xi_k}{m_k}}=\sum_{\xi} e^{2\pi i\frac{\xi}{m}}.$$

但是当 $\alpha_s=1$ 时,我們得出

$$\sum_{\xi_s} e^{2\pi i\frac{\xi_s}{m_s}}=\sum_{x_s} e^{2\pi i\frac{x_s}{m_s}}-1=-1.$$

当 $\alpha_s>1$时，讓 $m_s=p_s m_s'$, 我們得出

$$\sum_{\xi_s} e^{2\pi i\frac{\xi_s}{m_s}}=\sum_{x_s} e^{2\pi i\frac{x_s}{m_s}}-\sum_{u=0}^{m_s'-1} e^{2\pi i\frac{u}{m_s'}}=0.$$

b. 設 m 是整数, $m>1$。我們有 $\sum_{x=0}^{m-1} e^{2\pi i\frac{x}{m}}=0$。这个等式左边适合条件 $(x, m)=d$ 的各項的和，根据問題 a 的定理，等于 $\mu\left(\frac{m}{d}\right)$。

c. 我們得出

$$\sum_{\xi} e^{2\pi i\frac{\xi}{m}}=\sum_{d\backslash m}\mu(d)S_d,$$

这里,讓 $m=m_0 d$, 我們有

$$S_d=\sum_{u=0}^{m_0-1} e^{2\pi i\frac{u}{m_0}}.$$

后面的式子当 $d<m$ 时等于 0,而且当 $d=m$ 时等于 1。由此我們就得到問題 a 的定理。

d. 等式从問題 10, b 推出。

e. 我們有

$$A(m_1)\cdots A(m_k)=m^{-\tau}\sum_{a_1}\cdots\sum_{a_k}S_{a_1,\,m_1}\cdots S_{a_k,\,m_k},$$

这里 $a_1, \cdots, a_k$ 通过与模 $m_1, \cdots, m_k$ 互素的剩余組。由此問題里的第一个等式立刻可以推出(問題 d)。

用类似的方法可以証明第二个等式。

13, a. 我們有

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{nx}{p}}=\begin{cases}p, & \text{如果 } n \text{ 是 } p \text{ 的倍数,}\\ 0, & \text{其他情形。}\end{cases}$$

b. 把与給定的 n 对应的乘积展开,我們有

$$\sum_{d\diagdown a}\frac{\mu(d)}{d}\sum_{x=0}^{d-1} e^{2\pi i\frac{nx}{d}}.$$

由此,对所有的 $n=0, 1, \cdots, a-1$ 求总和,我們就得到关于 $\varphi(a)$的已知表示式。

14. 在右边的式子中,与除尽 a 的 x 对应的部分等于

$$\lim_{\varepsilon\to 0} 2\varepsilon\sum_{k=1}^{\infty}\frac{1}{k^{1+\varepsilon}}=\lim_{\varepsilon\to 0}\left(2\varepsilon\left(\int_1^{\infty}\frac{dx}{x^{1+\varepsilon}}+O(1)\right)\right)=2.$$

讓 $\Phi(K)=\sum\limits_{k=1}^{K} e^{2\pi i\frac{ak}{x}}$,則与不除尽 a 的 x 对应的部分可以表示成

$$\lim_{\varepsilon\to 0} 2\varepsilon\left(\frac{\Phi(1)}{1}+\frac{\Phi(2)-\Phi(1)}{2^{1+\varepsilon}}+\frac{\Phi(3)-\Phi(2)}{3^{1+\varepsilon}}+\cdots\right)=$$

$$=\lim_{\varepsilon\to 0} 2\varepsilon\left(\Phi(1)\left(1-\frac{1}{2^{1+\varepsilon}}\right)+\right.$$

$$\left.+\Phi(2)\left(\frac{1}{2^{1+\varepsilon}}-\frac{1}{3^{1+\varepsilon}}\right)+\cdots\right).$$

在 2^{ε} 后面的因子，由于 $|\Phi(K)|<x$，它的值 $<x$，然而 $\lim\limits_{\varepsilon\to 0} 2\varepsilon x=0$。所以問題里所說等式的右边，等于比 $\sqrt{a}$ 小的 a 的約数个数的兩倍再加上 δ，也就是等于 $\tau(a)$。

15, a. 我們有

$$(h_1+h_2)^p=h_1^p+\binom{p}{1}h_1^{p-1}h_2+\cdots$$

$$\cdots+\binom{p}{p-1}h_1h_2^{p-1}+h_2^p\equiv h_1^p+h_2^p \pmod p;$$

$$(h_1+h_2+h_3)^p\equiv(h_1+h_2)^p+h_3^p\equiv h_1^p+h_2^p+h_3^p \pmod p,$$

等等。

b. 讓 $h_1=h_2=\cdots=h_a=1$，从問題 a 的定理我們得到弗兒馬定理。

c. 設 $(a, p)=1$。对于某些整数 $N_1, N_2\cdots, N_\alpha$，我們有

$$a^{p-1}=1+N_1p,\ a^{p(p-1)}=(1+N_1p)^p=1+N_2p^2,$$

$$a^{p^2(p-1)}=1+N_3p^3,\ \cdots,\ a^{p^{\alpha-1}(p-1)}=1+N_\alpha p^\alpha,$$

$$a^{\varphi(p^\alpha)}\equiv 1 \pmod{p^\alpha}.$$

設 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解式。我們有

$$a^{\varphi(p_1^{\alpha_1})}\equiv 1 \pmod{p_1^{\alpha_1}},\ \cdots,\ a^{\varphi(p_k^{\alpha_k})}\equiv 1 \pmod{p_k^{\alpha_k}},$$

$$a^{\varphi(m)}\equiv 1 \pmod{p_1^{\alpha_1}},\ \cdots,\ a^{\varphi(m)}\equiv 1 \pmod{p_k^{\alpha_k}},$$

$$a^{\varphi(m)}\equiv 1 \pmod m.$$

第四章

1, a. 这定理可以直接从第三章問題 11, a 的定理推出。

b. 設 d 是 m 的約数，$m=m_0d$，H_d 表示問題 a 里 Tm 的表示式中有条件 $(a, m)=d$ 的各項的总和。我們得出

$$H_d=\sum_{a_0}\sum_{x=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{a_0f(x,\cdots,w)}{m_0}},$$

这里 a_0 通过与模 m_0 互素的剩余組。由此我們引出

$$H_d=d^r\sum_{a_0}\sum_{x_0=0}^{m_0-1}\cdots\sum_{w_0=0}^{m_0-1}\quad e^{2\pi i\frac{a_0f(x_0,\cdots,w_0)}{m_0}}=m^rA(m_0).$$

c. 設 $m>0$, $(a,m)=d$, $a=a_0d$, $m=m_0d$, T 是同余式 $ax\equiv b\pmod m$ 的解答的个数。我們有

$$Tm=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}\quad e^{2\pi i\frac{\alpha(ax-b)}{m}}=$$

$$=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}\quad e^{2\pi i\frac{\alpha a_0}{m_0}x-2\pi i\frac{b\alpha}{m}}=$$

$$=m\sum_{\alpha_1=0}^{d-1}\quad e^{-2\pi i\frac{b\alpha_1}{d}}=\begin{cases}md, & \text{如果 } b \text{ 是 } d \text{ 的倍数},\\ 0, & \text{其他情形。}\end{cases}$$

d. 假設 $(a,m)=d_1$, $(b,d_1)=d_2$, $\cdots$, $(f,d_{r-1})=d_r$, $m=d_1m_1$, $d_1=d_2m_2$, $\cdots$, $d_{r-1}=d_rm_r$ 我們得出 $d=d_r$,

$$Tm=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_1(ax+by+\cdots+fw+g)}{m}}=$$

$$=m\sum_{\alpha_1=0}^{d_1-1}\sum_{y=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_1(by+\cdots+fw+g)}{d_1}}=$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$=m^{r-1}\sum_{\alpha_{r-1}=0}^{d_{r-1}-1}\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_{r-1}(fw+g)}{d_{r-1}}}=m^r\sum_{\alpha_r=0}^{d_r-1}e^{2\pi i\frac{\alpha_rg}{d_r}}.$$

e. 我們用归納法来証明。設在問題 d 的記号下定理对于 r 个变数眞实了。討論同余式

$$lv+ax+\cdots+fw+g\equiv 0(\mathrm{mod}\ m). \qquad (2)$$

設 $(l,m)=d_0$。同余式(2)成立的条件是 $ax+\cdots+fw+g\equiv 0(\mathrm{mod}\ d_0)$。后一个同余式只有当 g 是 $d'=(a,\cdots,f,d_0)=(l,a,\cdots,f,m)$ 的倍数时才能成立，并且这时它有 $d_0^{r-1}d'$ 个解答。因此同余式(2)也只有在 g 是 d' 的倍数时才能成立，而且这时它有 $d_0^{r-1}d'\left(\frac{m}{d_0}\right)^r d_0=$ $=m^r d'$ 个解答。这样一来定理对于 $r+1$ 个变数也眞实了。但是定理对于一个变数眞实。所以它总是眞实的。

2, a. 我們有 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$, $a\cdot b\cdot a^{\varphi(m)-1}\equiv b(\mathrm{mod}\ m)$。

b. 我們有

$$1\cdot 2\cdots(a-1)ab(-1)^{a-1}\frac{(p-1)\cdots(p-a+1)}{1\cdot 2\cdots a}\equiv$$

$$\equiv b\cdot 1\cdot 2\cdots(a-1)(\mathrm{mod}\ p),$$

由此，兩边用 $1\cdot 2\cdots(a-1)$ 除，我們得到所說的定理。

c, α) 很明显地，只要限于 $(2,b)=1$ 的情形就够了。适当地选擇正負号，我們有 $b\pm m\equiv 0(\mathrm{mod}\ 4)$。設 2^δ 是除尽 $b\pm m$ 的 2 的最大乘方。对于 $\delta\geqslant k$，我們有

$$x\equiv\frac{b\pm m}{2^k}(\mathrm{mod}\ m).$$

而如果 $\delta<k$，則我們有

$$2^{k-\delta}x\equiv\frac{b\pm m}{2^\delta}(\mathrm{mod}\ m).$$

对于这个同余式再做同样的运算，等等。

β) 不妨認为 $(3,b)=1$。适当地选擇正負号，我們有 $b\pm m\equiv$ $\equiv 0(\mathrm{mod}\ 3)$。設 3^δ 是除尽 $b\pm m$ 的 3 的最大乘方。对于 $\delta\geqslant k$，我們有

$$x \equiv \frac{b \pm m}{3^k} \pmod{m}.$$

而如果 $\delta < k$，則我們有

$$3^{k-\delta} x \equiv \frac{b \pm m}{3^\delta} \pmod{m}.$$

对于这个同余式再做同样的运算，等等。

γ）設 p 是 a 的素約数。从条件 $b+mt \equiv 0 \pmod{p}$ 找出 t。設 p^δ 是除尽 $(a, b+mt)$ 的 p 的最大乘方，而且設 $a=a_1p^\delta$。我們有

$$a_1 x \equiv \frac{b+mt}{p^\delta} \pmod{m}.$$

如果 $a_1>1$，則对于这个新的同余式再做同样的运算，等等。

上述的方法适宜于 p 是 a 的不大的素因子的情形。

3. 讓 $t=[\tau]$，写下同余式：

$$a \cdot 0 \equiv 0 \pmod{m},$$
$$a \cdot 1 \equiv y_1 \pmod{m},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a \cdot t \equiv y_t \pmod{m},$$
$$a \cdot 0 \equiv m \pmod{m}.$$

照右边数的增加的順序把这些同余式排好（参看第二章問題 4,a），再依次从后一同余式减去前一同余式，我們得到 $t+1$ 个形式 $az \equiv u \pmod{m}$ 的同余式；$0<|z|\leqslant\tau$。这时，至少在一个同余式里有 $0<u<\frac{m}{\tau}$。这是因为 u 有 $t+1>\tau$ 个表示法，它們都是正的，而且它們的总和等于 m。

4, a, α）从符号分数的定义推出。

β）这里可以假定 $b_0=b+mt$，这里 t 由条件 $b+mt\equiv 0 \pmod{a}$ 决定；于是适合同余式 $ax\equiv b \pmod{m}$ 的就是由通常的分数 $\frac{b_0}{a}$ 所表示的整数。

γ）我們有（b_0 是 a 的倍数，d_0 是 c 的倍数）

$$\frac{b}{a}+\frac{d}{c}\equiv\frac{b_0}{a}+\frac{d_0}{c}\equiv\frac{b_0c+ad_0}{ac}\equiv\frac{bc+ad}{ac}.$$

δ) 我們有

$$\frac{b}{a}\cdot\frac{d}{c}\equiv\frac{b_0}{a}\cdot\frac{d_0}{c}\equiv\frac{b_0d_0}{ac}\equiv\frac{bd}{ac}.$$

b, α) 我們有(同余式取模 p)

$$\binom{p-1}{a}=\frac{(p-1)(p-2)\cdots(p-a)}{1\cdot2\cdots a}\equiv\frac{(-1)^a1\cdot2\cdots a}{1\cdot2\cdots a}\equiv(-1)^a.$$

从問題 2, b 現在很容易解出:

$$\frac{b}{a}\equiv\frac{b(-1)^{a-1}(p-1)\cdots(p-(a-1))}{1\cdot2\cdots(a-1)a}\pmod p.$$

β) 我們有

$$\frac{2^p-2}{p}\equiv1+\frac{p-1}{1\cdot2}+\frac{(p-1)(p-2)}{1\cdot2\cdot3}+\cdots+$$
$$+\frac{(p-1)(p-2)\cdots(p-(p-2))}{1\cdot2\cdots(p-1)}\pmod p.$$

5, a. 数 $s, s+1, \cdots, s+n-1$ 的每一对都不能与 d 有大于 1 的公約数。因为把 d 分成 n 个兩兩互素的因子（考慮到它們的次序)的方法有 n^k 个(第二章問題 11, b)。把乘积 $s(s+1)\cdots(s+n-1)$ 与这 n^k 个集合結合起来看。設 $d=u_1u_2\cdots u_n$ 是这样分法的一个。則适合条件 $s\equiv0\pmod{u_1}, s+1\equiv0\pmod{u_2}, \cdots, s+n-1\equiv0\pmod{u_n}$ 的乘积的个数等于 $\frac{a}{d}$。所以所求的数等于 $n^k\frac{a}{d}$。

b. 所說的个数等于

$$\sum_{d\diagdown a}\mu(d)S_d;\quad S_d=\frac{n^ka}{d},$$

这里 k 是 d 的不同的素約数的个数。但是我們有

$$\sum_{d\diagdown a}\mu(d)\frac{n^ka}{d}=a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\cdots\left(1-\frac{n}{p_k}\right).$$

6, a. 适合第一个同余式的所有 x, 給出等式 $x=b_1+m_1t$, 这里 t 是整数。为了在它們中間选取同时适合第二个同余式的 x, 只要限制在适合下面的同余式的 t 就成了:

$$m_1t\equiv b_2-b_1(\text{mod } m_2).$$

但是这个同余式能解在而且只在 b_2-b_1 是 d 的倍数时。在可解的情形下, 适合它的 t 的全部値, 由形式 $t=t_0+\frac{m_2}{d}t'$, 这里 t' 是整数, 的等式决定; 同时, 适合問題里所討論的組的 x 的全部値由下面的等式决定

$$x=b_1+m_1\left(t_0+\frac{m_2}{d}t'\right)=x_{1,2}+m_{1,2}t';\ x_{1,2}=b_1+m_1t_0.$$

b. 在同余式組

$$x\equiv b_1(\text{mod } m_1),\quad x\equiv b_2(\text{mod } m_2)$$

可解的情形下,适合它們的 x 的全部値由同余式 $x\equiv x_{1,2}(\text{mod } m_{1,2})$ 表示。在組

$$x\equiv x_{1,2}(\text{mod } m_{1,2}),\quad x\equiv b_3(\text{mod } m_3)$$

可解的情形下, 适合它們的 x 的全部値由同余式 $x\equiv x_{1,2,3}(\text{mod } m_{1,2,3})$ 表示。在組

$$x\equiv x_{1,2,3}(\text{mod } m_{1,2,3}),\quad x\equiv b_4(\text{mod } m_4)$$

可解的情形下, 适合它們的 x 的全部値由同余式 $x\equiv x_{1,2,3,4}$ $(\text{mod } m_{1,2,3,4})$ 表示, 等等。

7, α) 用 $-x$ 代替 x (結果 x' 也被 $-x'$ 代替了) 以后, 和数 $\left(\frac{a, b}{m}\right)$ 的値不变。

β) 当 x 通过与模 m 互素的剩余組时, x' 也通过与模 m 互素的剩余組。

γ) 假設 $x\equiv hz(\text{mod } m)$, 我們得到

$$\left(\frac{a, bh}{m}\right)=\sum_{z} e^{2\pi i\frac{ahz+bz'}{m}}=\left(\frac{ah, b}{m}\right).$$

δ）我們有

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right)=\sum_{x}\sum_{y} e^{2\pi i\frac{a_1m_2x+a_2m_1y+m_2x'+m_1y'}{m_1m_2}}.$$

假設 $m_2x'+m_1y'=z'$, 我們有

$$(a_1m_2x+a_2m_1y)(m_2x'+m_1y')\equiv a_1m_2^2+a_2m_1^2 \pmod{m_1m_2,}$$

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right)=\left(\frac{m_2^2a_1+m_1^2a_2, 1}{m_1m_2}\right),$$

这証明了在兩个因子的情形下的所說性質。推广到多于兩个因子的情形是显然的。

8. 同余式

$$a_0x^n+a_1x^{n-1}+\cdots+a_n-a_0(x-x_1)(x-x_2)\cdots(x-x_n)\equiv 0 \pmod p$$

有 n 个解答。它的次数低于 n。因此，它的所有系数都是 p 的倍数。这就是問題里的那些同余式所表示的。

9, a. 当 $p>3$ 时，与数列 $2, 3, \cdots, p-1$ 中取出的 x 对应，我們能在同一个数列里找到与它不同的 x', 适合条件 $xx'\equiv 1 \pmod p$; 实际上，从 $x=x'$ 推出 $(x-1)(x+1)\equiv 0 \pmod p$, $x=1$ 或者 $x=p-1$。所以

$$2\cdot 3\cdots(p-2)\equiv 1 \pmod p;\ 1\cdot 2\cdots(p-1)\equiv -1 \pmod p.$$

b. 設 $P>2$。假如 P 有約数 u 适合条件 $1<u<P$, 我們就有

$$1\cdot 2\cdots(P-1)+1\equiv 1 \pmod u.$$

10, a. 找出有条件 $a_0h\equiv 1 \pmod m$ 的 h。所給的同余式就等价于:

$$x^n+a_1hx^{n-1}+\cdots+a_nh\equiv 0 \pmod m.$$

b. 設 $Q(x)$ 和 $R(x)$ 分別是 x^p-x 被 $f(x)$ 除的商数和余数。

$Q(x)$ 和 $R(x)$ 的所有系数都是整数，$Q(x)$ 的次数是 $p-n$，$R(x)$ 的次数低于 n，

$$x^p-x=f(x)Q(x)+R(x).$$

設同余式 $f(x)\equiv 0 \pmod p$ 有 n 个解答。則这些解答也是 $R(x)\equiv 0 \pmod p$ 的解答；所以 $R(x)$ 的所有系数都是 p 的倍数。

反之，設 $R(x)$ 的所有系数都是 p 的倍数。那末对于 x 的同一些值，当 $f(x)Q(x)$ 是 p 的倍数时，x^p-x 也是 p 的倍数；所以下面兩个同余式

$$f(x)\equiv 0 \pmod p,\quad Q(x)\equiv 0 \pmod p$$

的解答的总数不小于 p。設第一个同余式有 α 个解答，第二个有 β 个解答。从

$$\alpha\leqslant n,\ \beta\leqslant p-n,\ p\leqslant \alpha+\beta.$$

我們引出 $\alpha=n,\ \beta=p-n$。

c. 把已知同余式兩边自乘 $\frac{p-1}{n}$ 次，得出所說条件的必要性。

設这个条件成立了；从 $x^p-x=x(x^{p-1}-A^{\frac{p-1}{n}}+A^{\frac{p-1}{n}}-1)$ 推出 x^p-x 被 x^n-A 除的余数是 $(A^{\frac{p-1}{n}}-1)x$；这里 $A^{\frac{p-1}{n}}-1$ 是 p 的倍数。

11. 从 $x_0^n\equiv A \pmod m$，$y^n\equiv 1 \pmod m$ 推出 $(x_0y)^n\equiv A \pmod m$；这时与互相不同余的 y（对于模 m 說）对应的乘积 x_0y 也互相不同余。从 $x_0^n\equiv A \pmod m$，$x^n\equiv A \pmod m$ 推出 $x^n\equiv x_0^n \pmod m$，并且在用条件 $x\equiv yx_0 \pmod m$ 来决定 y 后，我們就有 $y^n\equiv 1 \pmod m$。

第五章

1. 所說的同余式等价于 $(2ax+b)^2\equiv b^2-4ac \pmod m$。与同

余式$z^2\equiv b^2-4ac \pmod m$的每个解答$z\equiv z_0 \pmod m$对应，从$2ax+$ $+b\equiv z_0 \pmod m$，我們可以找出所說同余式的一个解答。

2, a. 对于$\left(\frac{a}{p}\right)=1$，我們有$a^{2m+1}\equiv 1 \pmod p$，$(a^{m+1})^2\equiv$ $\equiv a \pmod p$，$x\equiv\pm a^{m+1} \pmod p$。

b. 对于$\left(\frac{a}{p}\right)=1$，我們有$a^{4m+2}\equiv 1 \pmod p$，$a^{2m+1}\equiv\pm 1 \pmod p$，$a^{2m+2}\equiv\pm a \pmod p$。由于$\left(\frac{2}{p}\right)=-1$，我們还有$2^{4m+2}\equiv -1 \pmod p$。所以有某个等于0或者1的$s$，使我們得到

$$a^{2m+2}2^{(4m+2)s}\equiv a \pmod p,\ x\equiv\pm a^{m+1}2^{(2m+1)s} \pmod p.$$

c. 設$p=2^kh+1$，这里$k\geqslant 3$而且h是單数，$\left(\frac{a}{p}\right)=1$。我們有

$$a^{2^{k-1}h}\equiv 1 \pmod p,\ a^{2^{k-2}h}\equiv\pm 1 \pmod p,\ N^{2^{k-1}h}\equiv -1 \pmod p.$$

所以有某个非負的整数s_2，使我們得到

$$a^{2^{k-2}h}N^{s_2 2^{k-1}}\equiv 1 \pmod p,\ a^{2^{k-3}h}N^{s_2 2^{k-2}}\equiv\pm 1 \pmod p;$$

由此就有某个非負的整数s_3，使我們得到

$$a^{2^{k-3}h}N^{s_3 2^{k-2}}\equiv 1 \pmod p,\quad a^{2^{k-4}h}N^{s_3 2^{k-3}}\equiv\pm 1 \pmod p;$$

等等；最后，我們得到

$$a^hN^{2s_k}\equiv 1 \pmod p,\ x\equiv\pm a^{\frac{h+1}{2}}N^{s_k} \pmod p.$$

d. 我們有

$$1\cdot 2\cdots 2m(p-2m)\cdots(p-2)(p-1)+1\equiv 0 \pmod p,$$

$$(1\cdot 2\cdots 2m)^2+1\equiv 0 \pmod p.$$

3, a. 同余式(1)和(2)可解的条件很容易得出（§2, f和§2, k）。同余式(3)可解如果而且只如果$\left(\frac{-3}{p}\right)=1$。但是$\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$，并且

$$\left(\frac{p}{3}\right)=\begin{cases}1, \text{如果 } p \text{ 有形式 } 6m+1,\\ -1, \text{如果 } p \text{ 有形式 } 6m+5。\end{cases}$$

b. 对于形式 $4m+1$ 的任意不同的素数 $p_1, p_2, \cdots, p_k$, 数 $(2p_1p_2\cdots p_k)^2+1$ 的最小素約数 p, 与 $p_1p_2, \cdots, p_k$ 都不同，而且由于 $(2p_1p_2\cdots p_k)^2+1\equiv 0 \pmod p$, 它还有形式 $4m+1$。

c. 对于形式 $6m+1$ 的任意不同的素数 $p_1, p_2, \cdots, p_k$, 数 $(2p_1p_2\cdots p_k)^2+3$ 的最小素約数 p, 与 $p_1, p_2, \cdots, p_k$ 都不同，而且由于 $(2p_1p_2\cdots p_k)^2+3\equiv 0 \pmod p$, 它还有形式 $6m+1$。

4. 在第一个集合的数中間，有着与 $1\cdot 1, 2\cdot 2, \cdots, \frac{p-1}{2}\cdot\frac{p-1}{2}$ (也就是完全剩余組里所有的平方剩余)同余的数；按已知条件，这使得在第二个集合里只有平方非剩余了。但是在第二个集合里还有着这个平方非剩余和所有平方剩余的乘积，也就是說，那里有着所有的平方非剩余。

5, a. 設在 p 进位的計数系統里，

$$a=a_{\alpha-1}p^{\alpha-1}+\cdots+a_1p+a_0,$$

而且所求的解答(非負的最小剩余)是

$$x=x_{\alpha-1}p^{\alpha-1}+\cdots+x_1p+x_0.$$

造出下面的表:

$a_{\alpha-1}$	$\cdots$	a_4	a_3	a_2	a_1	a_0
$2x_0x_{\alpha-1}$	$\cdots$	$2x_0x_4$	$2x_0x_3$	$2x_0x_2$	$2x_0x_1$	x_0^2
$2x_1x_{\alpha-2}$	$\cdots$	$2x_1x_3$	$2x_1x_2$	x_1^2		
$2x_2x_{\alpha-3}$	$\cdots$	x_2^2				
$\cdots$						

这里在直行 a_s 下面的数的总和，表示(1)式右边平方以后对 p 的展开式中 p^s 項的系数。我們从条件

$$x_0^2\equiv a_0 (\bmod p)$$

求出 x_0。讓 $\frac{x_0^2-a_0}{p}=p_1$, 我們从条件

$$p_1+2x_0x_1\equiv a_1 (\bmod p)$$

求出 x_1。讓 $\frac{p_1+2x_0x_1-a_1}{p}=p_2$, 我們从条件

$$p_2+2x_0x_2+x_1^2\equiv a_2 (\bmod p),$$

求出 x_2, 等等。对于已知的 x_0, 由于 $(x_0, p)=1$, 数 $x_1, x_2, \cdots, x_{\alpha-1}$ 都唯一决定。

b. 这里

$$a=a_{\alpha-1}2^{\alpha-1}+\cdots+a_32^3+a_22^2+a_12+a_0,$$

$$x=x_{\alpha-1}2^{\alpha-1}+\cdots+x_32^3+x_22^2+x_12+x_0,$$

而且我們有下面的表:

$a_{\alpha-1}$	$\cdots$	a_4	a_3	a_2	a_1	a_0
$x_0x_{\alpha-2}$	$\cdots$	x_0x_3	x_0x_2	x_0x_1		x_0^2
$x_1x_{\alpha-3}$	$\cdots$	x_1x_2		x_1^2		
$x_2x_{\alpha-4}$	$\cdots$	x_2^2				
$\cdots$						

只考虑 $\alpha\geqslant 3$ 的情形。由于 $(a, 2)=1$, 必須 $a_0=1$。所以 $x_0=1$。再有, 必須 $a_1=0$, 而且由于 $x_0x_1+x_1^2=x_1+x_1^2\equiv 0 (\bmod 2)$, 必須 $a_2=0$。关于 x_1 有兩个可能的值: 0 和 1。数 $x_2, x_3, \cdots, x_{\alpha-2}$ 是唯一决定的, 而关于 $x_{\alpha-1}$ 又有兩个可能的值: 0 和 1。所以对于 $\alpha\geqslant 3$ 必須 $a\equiv 1 (\bmod 8)$, 而且这时所說的同余式有四个解答。

6. 明显地, P 和 Q 都是整数, 并且 Q 与我們用 z^2 来代替 a (也就是用 z 来代替 $\sqrt{a}$) 而得到的数同余。所以 $Q\equiv 2^{\alpha-1}z^{\alpha-1}$(mod

p);因此 $(Q,p)=1$,而且 Q' 确实可以由同余式 $QQ'\equiv 1 \pmod{p^\alpha}$ 定出。于是我們有

$$P^2-aQ^2=(z+\sqrt{a})^\alpha(z-\sqrt{a})^\alpha=(z^2-a)^\alpha\equiv 0 \pmod{p^\alpha},$$

由此 $$(PQ')^2\equiv a(QQ')^2\equiv a \pmod{p^\alpha}.$$

7. 設 $m=2^\alpha p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解式。于是把 m 表示成 $m=2^\alpha ab, (a,b)=1$ 共有 2^k 种方法。

設 $\alpha=0$。从 $(x-1)(x+1)\equiv 0 \pmod m$ 推出,对于某兩个 a 和 b

$$x\equiv 1 \pmod a;\quad x\equiv -1 \pmod b.$$

解这个組,我們得到一个解答 $x\equiv x_0 \pmod m$。所以所說同余式有 2^k 个解答。

設 $\alpha=1$。对于某兩个 a 和 b,

$$x\equiv 1 \pmod{2a};\quad x\equiv -1 \pmod{2b}.$$

解这个組,我們得到一个解答 $x\equiv x_0 \pmod m$。所以所說同余式有 2^k 个解答。

設 $\alpha=2$。对于某兩个 a 和 b,

$$x\equiv 1 \pmod{2a};\quad x\equiv -1 \pmod{2b}.$$

解这个組,我們得到一个解答 $x\equiv x_0\left(\bmod \frac{m}{2}\right)$。所以所說同余式有 2^{k+1} 个解答。

設 $\alpha\geqslant 3$。对于某兩个 a 和 b,下面兩組同余式都应該成立:

$$x\equiv 1 \pmod{2a};\qquad x\equiv -1 \pmod{2^{\alpha-1}b},$$

$$x\equiv 1 \pmod{2^{\alpha-1}a};\quad x\equiv -1 \pmod{2b}.$$

解每个組我們都得到一个解答 $x\equiv x_0\left(\bmod \frac{m}{2}\right)$。所以所說同余式有 2^{k+2} 个解答。

8, a. 用同余式 $xx'\equiv 1 \pmod p$ 定出 x',我們有

$$\sum_{x=1}^{p-1}\left(\frac{x(x+k)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{xx'(xx'+kx')}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{1+kx'}{p}\right).$$

明显地，$1+kx'$ 通过完全剩余組里所有的剩余，除去 1。由此推出所說的定理。

b. 所說等式从下面的式子推出：

$$T=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)\right)\left(1+\eta\left(\frac{x+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)+\eta\left(\frac{x+1}{p}\right)+\varepsilon\eta\left(\frac{x(x+1)}{p}\right)\right).$$

c. 我們有

$$S\leqslant X\sum_{x=0}^{p-1}\sum_{y_1}\sum_{y}\left(\frac{(xy_1+k)(xy+k)}{p}\right).$$

这式子右边 $y=y_1$ 的部分不超过 XpY。我們来討論 y 不等于 y_1 的那一部分，并且为了确定起見，假定 $y>0$。讓 $xy+k\equiv z \pmod p$，把所說的部分化成

$$X\sum_{z=0}^{p-1}\left(\frac{z\left(\frac{y_1}{y}z+k\left(1-\frac{y_1}{y}\right)\right)}{p}\right).$$

由此肯定这式子的数値 $\leqslant X$（問題 a）。所以

$$S^2<XpY+XY^2\leqslant 2pXY.$$

d, α) 我們有

$$S=\sum_{x=0}^{p-1}\sum_{z_1=0}^{Q-1}\sum_{z=0}^{Q-1}\left(\frac{(x+z_1)(x+z)}{p}\right).$$

当$z_1=z$时，对x求总和，給出$p-1$。当z_1不等于z时，对x求总和，給出-1(問題a)。所以

$$S=(p-1)Q-Q(Q-1)=(p-Q)Q.$$

β) 根据問題α的定理，我們有

$$T(Q^{0.5+0.5\lambda})^2<pQ;\quad T<pQ^{-\lambda}.$$

γ) 讓$[\sqrt{p}]=Q$，应用問題α的定理。假如在問題里所說的数列中沒有平方非剩余，那末对于$x=M, M+1, \cdots, M+2Q-1$，有$|S_x|\geqslant Q-1$，而这样一来，

$$2Q(Q-1)^2\leqslant(p-Q)Q,\quad 2(Q-1)^2\leqslant(Q+1)^2-Q,\quad Q^2-5Q<0.$$

对于$Q\geqslant 5$，这是不可能的。

9, a. 如果m表示成(1)的形式，則同余式$x\equiv zy \pmod m$的解答

$$z\equiv z_0 \pmod m \tag{5}$$

也是同余式(2)的解答。我們就說，所說的表示式与同余式(2)的解答(5)相关。

与同余式(2)的每个解答(5)相关的至少有一个表示式(1)。实际上，取$\tau=\sqrt{m}$，我們有

$$\frac{z_0}{m}=\frac{P}{Q}+\frac{\theta}{Q\sqrt{m}};\quad (P, Q)=1,\quad 0<Q\leqslant\sqrt{m},\quad |\theta|<1.$$

所以$z_0Q=mP+r$，这里$|r|<\sqrt{m}$。再有，从(2)推出$|r|^2+Q^2\equiv$ $\equiv 0 \pmod m$。由此再从$0<|r|^2+Q^2<2m$，我們得出

$$m=|r|^2+Q^2. \tag{6}$$

这时$(|r|, Q)=1$，由于

$$1=\frac{r^2+Q^2}{m}=\frac{(z_0Q-mP)z_0Q-rmP+Q^2}{m}\equiv -rP \pmod Q.$$

如果$|r|=r$，則由于$r\equiv z_0Q \pmod m$，表示式(6)与解答(5)相关。如果$|r|=-r$，則由于$z_0^2Q\equiv z_0r \pmod m$，$Q\equiv z_0|r| \pmod m$，表示

式(6)还与解答(5)相关。

与每个解答(5)相关的至多有一个表示式(1)。因为，如果有兩个表示式 $m=x^2+y^2$ 和 $m=x_1^2+y_1^2$ 把 m 表示成(1)的形式，而且与同一个解答(5)相关，则从 $x\equiv z_0y \pmod m$, $x_1\equiv z_0y_1 \pmod m$ 推出 $xy_1\equiv x_1y \pmod m$。所以 $xy_1=x_1y$, 于是根据 $(x,y)=(x_1,y_1)=1$ 推出 $x=x_1$, $y=y_1$。

b. 如果 m 表示成形式(3)，则同余式 $x\equiv zy \pmod p$ 的解答

$$z\equiv z_0 \pmod p \tag{7}$$

也是同余式(4)的解答。我們就說，所說表示式与同余式(4)的解答(7)相关。

知道了同余式(4)的解答(7)，我們至少可以找出一个表示式(3)。实际上，取 $\tau=\sqrt{p}$, 我們有

$$\frac{z_0}{p}=\frac{P}{Q}+\frac{\theta}{Q\sqrt{p}};\quad (P,Q)=1,\quad 0<Q\leqslant\sqrt{p},\quad |\theta|<1.$$

所以 $z_0Q\equiv r \pmod p$, 这里 $|r|<\sqrt{p}$。再有从(4)式推出 $|r|^2+aQ^2\equiv$ $\equiv 0 \pmod p$。由此再从 $0<|r|^2+aQ^2<(1+a)p$ 推出，对于 $a=2$, 应該有 $|r|^2+2Q^2=p$ 或者 $|r|^2+2Q^2=2p$。在后一情形 $|r|$ 是偶数，$|r|=2r_1$, $p=Q^2+2r_1^2$。对于 $a=3$ 应該有 $|r|^2+3Q^2=p$, 或者 $|r|^2+3Q^2=2p$, 或者 $|r|^2+3Q^2=3p$。第二种情形不可能：对于模4, 左边与0同余而右边则与2同余。在第三种情形 $|r|$ 是3的倍数，$|r|=3r_1$, $p=Q^2+3r_1^2$。

假如有两个表示式 $p=x^2+ay^2$ 和 $p=x_1^2+ay_1^2$, 把 p 表示成形式(3)，而且与同余式(4)的同一个解答相关，我們会得出 $x=x_1$, $y=y_1$。假如这兩个表示式与同余式(4)的不同的解答相关，我們得出 $x\equiv zy \pmod p$, $x_1\equiv -zy_1 \pmod p$, 于是 $xy_1+x_1y\equiv 0 \pmod p$, 由于 $0<(xy_1+x_1y)^2\leqslant(x^2+y^2)(x_1^2+y_1^2)<p^2$, 这是不可能的。

c, α) 和式 $S(k)$ 的各項对于 $x=x_1$ 和 $x=-x_1$ 有相等的值。

β) 我們有

$$S(kt^2)=\sum_{x=0}^{p-1}\left(\frac{xt(x^2t^2+kt^2)}{p}\right)=\left(\frac{t}{p}\right)S(k).$$

γ) 讓 $p-1=2p_1$, 我們有

$$p_1(S(r))^2+p_1(S(n))^2=\sum_{t=1}^{p_1}(S(rt^2))^2+\sum_{t=1}^{p_1}(S(nt^2))^2=$$

$$=\sum_{k=1}^{p-1}(S(k))^2=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)\ (y^2+k)}{p}\right).$$

对不等于 x 或者 $p-x$ 的 y, 对 k 求总和的結果是 $-2\left(\frac{xy}{p}\right)$; 对于 $y=x$ 或者 $y=p-x$, 它是 $(p-2)\left(\frac{xy}{p}\right)$。所以

$$p_1(S(r))^2+p_1(S(n))^2=4pp_1,\ \ p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2.$$

10, a. 我們有

$X^2-DY^2=$

$$=(x_1+y_1\sqrt{D})\ (x_2\pm y_2\sqrt{D})\ (x_1-y_1\sqrt{D})\ (x_2\mp y_2\sqrt{D})=$$
$$=k^2。$$

b. 取任意的 $\tau_1>1$, 我們求出有条件 $|y_1\sqrt{D}-x_1|<\frac{1}{\tau_1}$, $0<<y\leqslant\tau_1$ 的整数 x_1, y_1, 再把它逐項乘到 $y_1\sqrt{D}+x_1<2y_1\sqrt{D}+1$ 上, 我們得到 $|x_1^2-Dy_1^2|<2\sqrt{D}+1$。取 $\tau_2>\tau_1$ 适合条件 $|y_1\sqrt{D}-x_1|>\frac{1}{\tau_2}$, 我們再求出有条件 $|x_2^2-Dy_2^2|<2\sqrt{D}+1$ 的整数 x_2, y_2, 等等。

明显地, 在間隔 $-2\sqrt{D}-1<k<2\sqrt{D}+1$ 里存在着不等于零的整数 k, 使得数偶 $x_1, y_1; x_2, y_2; \cdots$ 中間有無数对 x, y 适合条件 $x^2-Dy^2=k$; 在后者中間还一定有兩对 ξ_1, η_1 和 ξ_2, η_2 适合条件

$\xi_1\equiv\xi_2 \pmod{|k|}$, $\eta_1\equiv\eta_2 \pmod{|k|}$。用等式 $\xi_0+\eta_0\sqrt{D}=(\xi_1+\eta_1\sqrt{D})(\xi_2-\eta_2\sqrt{D})$ 定出整数 ξ_0, η_0, 我們有(問題 a)

$$\xi_0^2-D\eta_0^2=|k|^2;\quad \xi_0\equiv\xi_1^2-D\eta_1^2\equiv 0 \pmod{|k|};$$

$$\eta_0\equiv-\xi_1\eta_1+\xi_1\eta_1\equiv 0 \pmod{|k|}.$$

所以 $\xi_0=\xi|k|$, $\eta_0=\eta|k|$, 这里 ξ 和 η 都是整数而且 $\xi^2-D\eta^2=1$。

c. 由等式(2)所定的数 x, y 适合方程(1)(問題 a)。

假如有适合方程(1), 但是与(2)式所定的数偶不同的正整数偶存在,我們对于某个 $r=1, 2, \cdots$ 就有

$$(x_0+y_0\sqrt{D})^r<x+y\sqrt{D}<(x_0+y_0\sqrt{D})^{r+1}.$$

由此,逐項用 $(x_0+y_0\sqrt{D})^r$ 除,我們得到

$$1<X+Y\sqrt{D}<x_0+y_0\sqrt{D}, \qquad (3)$$

这里 X 和 Y 由等式

$$X+Y\sqrt{D}=\frac{x+y\sqrt{D}}{(x_0+y_0\sqrt{D})^r}=(x+y\sqrt{D})(x_0-y_0\sqrt{D})^r$$

定出,都是整数,而且适合方程(問題 a)

$$X^2-DY^2=1. \qquad (4)$$

但是从(4)式推出不等式 $0<|X|-|Y\sqrt{D}|<1$, 这与(3)式的第一个不等式結合起来指出 X 和 Y 都是正的。所以(3)式的第二个不等式与 x_0 和 y_0 的定义矛盾。

11, a, α) 我們有

$$|U_{a,p}|^2=U_{a,p}\overline{U}_{a,p}=\sum_{t=1}^{p-1}\sum_{x=1}^{p-1}\left(\frac{t}{p}\right)e^{2\pi i\frac{ax(t-1)}{p}}.$$

对于 $t=1$, 对 x 求总和給出 $p-1$; 对于 $t>1$, 它給出 $-\left(\frac{t}{p}\right)$。所以

$$|U_{a,p}|^2=p-1-\sum_{t=2}^{p-1}\left(\frac{t}{p}\right)=p,\quad |U_{a,p}|=\sqrt{p},$$

或者

$$|U_{a,p}|^2=U_{a,p}\overline{U}_{a,p}=\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x+t}{p}\right)\left(\frac{x}{p}\right)e^{2\pi i\frac{at}{p}}.$$

对于$t=0$, 对 x 求总和給出 $p-1$; 对于 $t>0$, 它給出 $-e^{2\pi i\frac{at}{p}}$。所以

$$|U_{a,p}|^2=p-1-\sum_{t=1}^{p-1}e^{2\pi i\frac{at}{p}}=p,\quad |U_{a,p}|=\sqrt{p}.$$

β) 对于$(a,p)=p$, 定理是显然的。对于$(a,p)=1$, 它从下面的式子推出

$$U_{a,p}=\frac{a}{p}\sum_{x=1}^{p-1}\left(\frac{ax}{p}\right)e^{2\pi i\frac{ax}{p}}=\left(\frac{a}{p}\right)U_{1,p}.$$

b, α) 設 r 和 n 分别通过完全剩余組里的平方剩余和平方非剩余。我們有

$$S_{a,p}=1+2\sum_{r}e^{2\pi i\frac{ar}{p}}.$$

把它与

$$0=1+\sum_{r}e^{2\pi i\frac{ar}{p}}+\sum_{n}e^{2\pi i\frac{an}{p}}$$

相减,我們就得到所說等式。

β) 我們有

$$|S_{a,m}|^2=\sum_{t=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi i\frac{a(t^2+2tx)}{m}}.$$

对于給定的 t, 对 x 求总和給出 $me^{2\pi i\frac{at^2}{m}}$ 或者 0, 就看 $2t$ 能否被 m 除尽。对于奇数 m, 我們有

$$|S_{a,m}|^2=me^{2\pi i\frac{a\cdot 0^2}{m}}=m.$$

对于偶数 $m=2m_1$ 我們有

$$|S_{a,m}|^2=m\left(e^{2\pi i\frac{a\cdot 0^2}{m}}+e^{2\pi i\frac{a\cdot m_1^2}{m}}\right).$$

这里右边对于奇数m_1等于零,而对于偶数 m_1 则等于 $2m$。

γ) 对于任意整数 b, 我們有

$$|S_{A,m}|=\left|\sum_{x=0}^{m-1}e^{2\pi i\frac{Ax^2+2Abx}{m}}\right|,$$

于是从条件 $2Ab\equiv a \pmod m$ 取 b, 我們就得到所說的結果 (問題 β)。

12, a. 我們有

$$m{\sum_z}'\Phi(z)=\sum_z\sum_{s=M}^{M+Q-1}\sum_{a=0}^{m-1}\Phi(z)e^{2\pi i\frac{a(z-s)}{m}}.$$

在右边的和式中,与 $a=0$ 对应的部分等于 $Q\sum\limits_z\Phi(z)$; 与 a 的其余的值对应的部分(第三章問題 11, c)

$$<\Delta\sum_{a=1}^{m-1}\left|\sum_{s=M}^{M+Q-1}e^{2\pi i\frac{-as}{m}}\right|<\Delta m(\ln m-\delta).$$

b, α) 从問題 a 的定理和問題 11, a, α 的定理推出。

β) 問題 α 的不等式給出 $R-N=\theta\sqrt{p}\ln p$。此外, 显然有 $R+N=Q$。

γ) 从問題 11, b, β 的定理推出,如果我們讓 $m=p$, $\Phi(z)=1$, 并且讓 z 通过 $z=x^2$; $x=0, 1, \cdots, p-1$, 則問題 a 的定理的条件都有了。但是在 z 的值中間有一个数对于模 p 与 0 同余, 而且其余的数对于模 p 成对地与完全剩余組的每个平方剩余同余。所以

$$\sum_z{}' \Phi(z)=2R, \quad \sum_z \Phi(z)=p,$$

我們就得到
$$2R=\frac{Q}{p}p+\theta\sqrt{p}\ln p.$$

δ) 从問題 a 的定理和問題 11, b, γ 的定理推出。

ε) 从問題 δ 的定理推出，如果讓 $m=p$, $\Phi(z)=1$, 并且讓 z 通过 $z=Ax^2$; $x=M_0, M_0+1, \cdots, M_0+Q_0-1$, 則問題 a 的定理的条件都有了。所以

$$\sum_z{}' \Phi(z)=T, \sum_z \Phi(z)=Q_0.$$

于是就推出問題里所說的公式。

c. 和式中由适合 $\left(\frac{a}{p}\right)=1$ 的各項所組成的部分等于 $p(R^2+N^2)$，其余的部分等于 $-2pRN$。所以整个和式等于 $p(R-N)^2$。

和式中由适合 $a=0$ 的各項所組成的部分等于 0，其余的部分按数值小于(第三章問題 11, c)

$$\sum_{a=1}^{p-1}\left|\sum_{x=M}^{M+Q-1} e^{2\pi i\frac{ax}{p}}\right|\left|\sum_{a=1}^{p-1}\right|\sum_{y=M}^{M+Q-1} e^{2\pi i\frac{-a\alpha y}{p}}\left|<p^2(\ln p)^2.\right.$$

因此，

$$p(R-N)^2<p^2(\ln p)^2, \quad |R-N|<\sqrt{p}\ln p.$$

第 六 章

1, a. 如果 q 是奇素数而且 $a^p\equiv 1 \pmod q$，則 a 对于模 q 屬于方次数 $\delta=1$; p 的一个。对于 $\delta=1$ 我們有 $a\equiv 1 \pmod q$ 对于 $\delta=p$ 我們有 $q-1=2px$; x 是整数。

b. 如果 q 是奇素数而且 $a^p+1\equiv 0 \pmod q$，則 $a^{2p}\equiv 1 \pmod q$。所以 a 对于模 q 屬于方次数 $\delta=1, 2, p, 2p$ 的一个。$\delta=1$; p 的情

形都不可能。对于 $\delta=2$ 我們有 $a^2\equiv 1(\bmod q)$, $a+1\equiv 0(\bmod q)$。对于 $\delta=2p$ 我們有 $q-1=2px$; x 是整数。

c. $2px+1$ 形式的素数，例如 2^p-1 的素約数就是。設 $p_1, p_2, \cdots, p_k$ 是任意 k 个 $2px+1$ 形式的素数; 数 $(p_1p_2\cdots p_k)^p-1$ 有形式 $2px+1$ 的素約数，它与 $p_1, p_2, \cdots, p_k$ 都不同。

d. 如果 q 是素数而且 $2^{2^n}+1\equiv 0(\bmod q)$，則 $2^{2^{n+1}}\equiv 1(\bmod q)$。所以 2 对于模 q 屬于方次数 2^{n+1}, 因此 $q-1=2^{n+1}x$; x 是整数。

2. 明显地，a 对于模 a^n-1 屬于方次数 n。所以 n 是 $\varphi(a^n-1)$ 的約数。

3. a. 設在 k 次运算以后又出現原先的数列。很明显地，这样的 k 次运算与下面的方法等价: 在数列

$$1, 2, \cdots, n-1, n, n, n-1, \cdots, 2, 1, 2, \cdots,$$
$$\cdots, n-1, n, n, n-1, \cdots, 2, 1, 2, \cdots$$

里取出第 1, 第 $1+2^k$, 第 $1+2\cdot 2^k$, $\cdots$ 个位置的数。所以上面这个数列的第 $1+2^k$ 个位置应該是 2。因此，問題里所説的条件是必要的。但是它又是充分的，因为它使我們有下列对于模 $2n-1$ 的同余式:

$$1\equiv 1, \quad 1+2^k\equiv 0, \quad 1+2\cdot 2^k\equiv -1, \cdots$$

或者

$$1\equiv 1, \quad 1+2^k\equiv 2, \quad 1+2\cdot 2^k\equiv 3, \cdots$$

b. 解法与問題 a 类似。

4. 同余式 $x^\delta\equiv 1(\bmod p)$ 的解答屬于方次数 $\frac{\delta}{\delta'}$，这里 δ' 是 δ 的約数。同时 δ' 是 d 的倍数在而且只在 $x^{\frac{\delta}{d}}\equiv 1(\bmod p)$时。把 δ' 改写为 δ，而且取 $f=1$，我們得到 $S'=\sum_{d\diagdown\delta}\mu(d)S_d$，这里 S' 是所求的数而且 $S_d=\frac{\delta}{d}$。

5, a. 这里应該有 $\left(\frac{g}{2^n+1}\right)=-1$(§3; §5, c 的例子)。这个要求在 $g=3$ 时成立。

b. 这里不应該有 $\left(\frac{g}{2p+1}\right)=1, g^2\equiv 1 \pmod{2p+1}$。这个要求对于所說的 g 成立。

c. 这里不应該有 $\left(\frac{g}{4p+1}\right)=1, g^4\equiv 1 \pmod{4p+1}$。这个要求在 $g=2$ 时成立。

d. 这里不应該有 $\left(\frac{g}{2^np+1}\right)=1, g^{2^n}\equiv 1 \pmod{2^np+1}$。这个要求在 $g=3$ 时成立。

6, a, α) 当 n 是 $p-1$ 的倍数时，定理显然真实。設 n 不被 $p-1$ 除尽，又設 g 是模 p 的元根。数 $1, 2, \cdots, p-1$，如果不考虑先后的順序，与数 $g, 2g, \cdots, (p-1)g$ 对于模 p 同余。所以

$$S_n\equiv g^nS_n \pmod p, \quad S_n\equiv 0 \pmod p.$$

β) 我們有

$$\sum_{x=1}^{p-1}\left(\frac{x(x^2+1)}{p}\right)\equiv\sum_{x=1}^{p-1}x^{\frac{p-1}{2}}(x^2+1)^{\frac{p-1}{2}} \pmod p,$$

于是我們就得到所說的結果(問題 α)。

b. 对于 $p>2$，我們有

$$1\cdot 2\cdots(p-1)\equiv g^{1+2+\cdots+p-1}\equiv g^{\frac{p-1}{2}}\equiv -1 \pmod p.$$

7, a. 我們有

$$g^{\operatorname{ind}_{g_1}a}\equiv a \pmod p, \quad \operatorname{ind}_{g_1}a \operatorname{ind}_g g_1\equiv \operatorname{ind}_g a \pmod{p-1},$$

$$\operatorname{ind}_{g_1}a\equiv\alpha \operatorname{ind}_g a \pmod{p-1}.$$

b. 从

$$\operatorname{ind}_g a\equiv s \pmod n, \quad \operatorname{ind}_{g_1}a\equiv\alpha \operatorname{ind}_g a \pmod{p-1},$$

推出 $$\mathrm{ind}_{g_1} a \equiv \alpha s \equiv s_1 \pmod{n}.$$

8. 設$(n, p-1)=1$。从条件 $nu\equiv 1 \pmod{p-1}$ 求出 u，我們得到解答 $x\equiv a^u \pmod{p}$。

設 n 是素数，$p-1=n^\alpha t$，α 是正整数，$(t,n)=1$。如果同余式成立，我們有 $a^{n^{\alpha-1}t}\equiv 1 \pmod{p}$；如果 $\alpha>1$，則由于 $x\equiv g^{n^{\alpha-1}tr} \pmod{p}$，$r=0, 1, \cdots, n-1$ 是 $x^n\equiv 1 \pmod{p}$ 的所有解答，对于某个 $r_1=0, 1, \cdots, n-1$，我們有

$$a^{n^{\alpha-2}t}g^{n^{\alpha-1}tr_1}\equiv 1 \pmod{p};$$

如果 $\alpha>2$，則对于某个 $r_2=0, 1, \cdots, n-1$，我們有

$$a^{n^{\alpha-3}t}g^{n^{\alpha-2}tr_1+n^{\alpha-1}tr_2}\equiv 1 \pmod{p},$$

等等；最后，对于某个 $r_{\alpha-1}=0, 1, \cdots, n-1$，…我們有

$$a^t g^{ntr_1+n^2tr_2+\cdots+n^{\alpha-1}tr_{\alpha-1}}\equiv 1 \pmod{p}.$$

从条件 $tu-nv=-1$ 求出 u 和 v，我們得到 n 个解答：

$$x\equiv a^v g^{ut(r_1+nr_2+\cdots+n^{\alpha-2}r_{\alpha-1})+n^{\alpha-1}tr} \pmod{p};\ r=0, 1, \cdots, n-1.$$

設素数 n_1 除尽 $(n, p-1)$，$n=n_1n_2$，$n_2>1$。与同余式 $y^{n_1}\equiv a \pmod{p}$ 的每个解答对应，我們找到同余式 $x^{n_2}\equiv y \pmod{p}$ 的解答。

9, a. 所說的方法使我們得到 $cc_0c_1\cdots c_k=\varphi(m)$ 个品格。設在兩个品格 $\chi_1(a)$ 和 $\chi_2(a)$ 里，根 $R, R_0, R_1, \cdots, R_k$ 中間有某一个的値 R' 和 R'' 彼此不相等；又設对于某个 a_1，所有的指数都等于 0，只有与 R' 和 R'' 对应的那一个等于 1，我們就有

$$\chi_1(a_1)=R', \quad \chi_2(a_1)=R''.$$

b. α) 我們有

$$\chi(1)=R^0\cdots R_k^0=1.$$

β) 設 $\gamma' \cdots, \gamma'_k$；$\gamma'', \cdots \gamma''_k$ 分別是 a_1 和 a_2 的指数組；那末

$\gamma'+\gamma'', \cdots, \gamma_k'+\gamma_k''$ 就是 a_1a_2 的指数組(§ 7, c)。

γ) 当 $a_1\equiv a_2 \pmod m$ 时，a_1 和 a_2 的各个指数对应地对于模 $c, \cdots, c_k$ 同余。

c. 所說性質从下面的式子推出:

$$\sum_{a=0}^{m-1}\chi(a)=\sum_{\gamma=0}^{c-1}R^{\gamma}\cdots\sum_{\gamma_k=0}^{c_k-1}R_k^{\gamma_k}.$$

d. 所說性質从下面的式子推出:

$$\sum_{\chi}\chi(a)=\sum_{R}R^{\gamma}\cdots\sum_{R_k}R_k^{\gamma_k}.$$

e. 設 $\psi(a_1)\gtrless 0$。那末 $\psi(a_1)=\psi(a_1)\psi(1)$。所以 $\psi(1)=1$。从条件 $aa'\equiv 1 \pmod m$ 求出 a'，我們有 $\psi(a)\psi(a')=1$。所以 $\psi(a)\gtrless 0$ 对于 $(a, m)=1$。

当 $(a_1, m)=1$ 时，我們有

$$\sum_a{}' \frac{\chi(a)}{\psi(a)}=\sum_a{}' \frac{\chi(a_1a)}{\psi(a_1a)}=\frac{\chi(a_1)}{\psi(a_1)}\sum_a{}' \frac{\chi(a)}{\psi(a)};$$

所以或者 $\sum_a{}' \frac{\chi(a)}{\psi(a)}=0$，或者对于所有的 a_1, $\psi(a_1)=\chi(a_1)$。但是第一种結論对于所有 χ 不能成立：那时將会有 $H=0$，可是 $H==\varphi(m)$。因为对于給定的 a，对所有品格求总和，我們有

$$\sum_{\chi}\frac{\chi(a)}{\psi(a)}=\begin{cases}\varphi(m), & \text{如果 } a\equiv 1 \pmod m,\\ 0, & \text{其余的情形。}\end{cases}$$

f, α) 如果 $R', \cdots, R_k'$ 和 $R'', \cdots, R_k''$ 是与品格 $\chi_1(a)$ 和 $\chi_2(a)$ 对应的 $R, \cdots, R_k$ 的値，則 $\chi_1(a)\chi_2(a)$ 也是品格，而且在它那里对应的値是 $R'R'', \cdots, R_k'R_k''$。

β) 当 $R, \cdots, R_k$ 通过对应的方程的所有根时，$R'R, \cdots, R_k'R_k$ 也以某个順序通过那些根。

γ）从条件 $ll' \equiv 1 \pmod m$ 定出 l'，我們有

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \sum_{\chi} \frac{\chi(al')}{\chi(ll')} = \sum_{\chi} \chi(al'),$$

它等于 $\varphi(m)$ 或者 0，就看同余式 $a \equiv l \pmod m$ 是否成立。

10, a, α）用同余式 $xx' \equiv 1 \pmod p$ 定出 x'，我們有

$$\sum_{x=1}^{p-1} e^{2\pi i \frac{l \operatorname{ind}(x+k) - l \operatorname{ind} x}{n}} = \sum_{x=1}^{p-1} e^{2\pi i \frac{l \operatorname{ind}(1+kx')}{n}} = -1.$$

β）我們有

$$S = \sum_{x=0}^{p-1} \sum_{z_1=0}^{Q-1} \sum_{z=0}^{Q-1} e^{2\pi i \frac{l \operatorname{ind}(x+z_1) - l \operatorname{ind}(x+z)}{n}}.$$

当 $z_1 = z$ 时，对 x 求总和給出 $p-1$，当 z_1 不等于 z 时，对 x 求总和給出 -1（問題 α）。所以

$$S = (p-1)Q - Q(Q-1) = (p-Q)Q.$$

γ）設 Q_x 是数列 $x+z$; $z = 0, 1, \cdots, Q-1$ 中不能被 p 除尽的数的个数，而 $T_{n,x}$ 則是同一个数列中屬于第 s 个集合的数的个数。最后，設

$$U_{n,x} = -\frac{Q_x}{n} + T_{n,x}, \quad S = \sum_{x=0}^{p-1} U_{n,x}^2.$$

我們有

$$U_{n,x} = \frac{1}{n} \sum_{l=1}^{n-1} \sum_{z=1}^{Q-1} e^{2\pi i \frac{l(\operatorname{ind}(x+z) - s)}{n}} = \frac{1}{n} \sum_{l=1}^{n-1} e^{-2\pi i \frac{ls}{n}} S_{l,n,x},$$

$$U_{n,x}^2 \leqslant \frac{1}{n^2}(n-1) \sum_{l=1}^{n-1} |S_{l,n,x}|^2, \quad S \leqslant \left(\frac{n-1}{n}\right)^2 (p-Q)Q.$$

讓 $Q = [n\sqrt{p}]$，而且假定在問題里所說的数列中沒有第 s 个集合

的数，我們就可以断定 $|U_{n,x}|\geqslant\frac{Q-1}{n}$ 对于 $x=M,M+1,\cdots,M+$ $+Q-1$，以致

$$Q\left(\frac{Q-1}{n}\right)^2\leqslant\left(\frac{n-1}{n}\right)^2(p-Q)Q,\quad (n\sqrt{p}-2)^2<(n\sqrt{p}-\sqrt{p})^2,$$

这是不可能的。

b. 設 p_0 是 $p-1$ 的不同的素約数的乘积，Q_x 是数列 $x+z$; $z=0,1,\cdots,Q-1$ 中不被 p 除尽的数的个数，而 G_x 則是同一个数列中模 p 的元根的个数。最后，設

$$P=\left(\sum_{d\backslash p_0}\frac{\mu(d)}{d}\right)^{-1}=\frac{p-1}{\varphi(p-1)},\quad w_x=-\frac{Q_x}{p}+G_x,\quad \Omega=\sum_{x=0}^{p-1}w_x^2.$$

取 $f(\xi)=1$，而且讓 ζ 通过 $\xi=\operatorname{ind}(x+z)$; $z=0,1,\cdots,Q-1$，我們得到 $S'=\sum_{d\backslash p_0}\mu(d)S_d$。这里 S' 是有条件 $(\xi,p-1)=1$ 的 ξ 的个数；所以 $S'=G_x$。再有 S_d 是倍于 d 的 ξ 的个数；所以当 $s=0$ 时，$S_d=T_{d,x}$(問題 a, γ)。因此

$$w_x=-\frac{Q_x}{p}+\sum_{d\backslash p_0}\mu(d)T_{d,x}=\sum_{d\backslash p_0}\mu(d)U_{d,x},$$

$$w_x^2\leqslant 2^k\sum_{d\backslash p_0}U_{d,x}^2,\ \Omega\leqslant 2^{2k}(p-Q)Q.$$

讓 $Q=[P2^k\sqrt{p}]$，而且假定在問題里所說的数列中沒有元根，我們就可以断定 $|w_x|\geqslant\frac{Q-1}{P}$ 对于 $x=M,M+1,\cdots,M+Q-1$，以致

$$Q\left(\frac{Q-1}{P}\right)^2\leqslant 2^{2k}(p-Q)Q,\ (P2^k\sqrt{p}-2)^2<\left(P2^k\sqrt{p}-\frac{p2^kQ}{2\sqrt{p}}\right)^2,$$

这是不可能的。

11, a, α) 我們有

$$|U_{a,p}|^2=\sum_{t=1}^{p-1}\sum_{x=1}^{p-1}e^{2\pi i\frac{k\,\mathrm{ind}\,t}{n}}e^{2\pi i\frac{a(t-1)x}{p}}=$$

$$=p-1-\sum_{t=2}^{p-1}e^{2\pi i\frac{k\,\mathrm{ind}\,t}{n}}=p.$$

β) 当 $(a, p)=p$ 时，定理显然真实。当 $(a, p)=1$ 时，它从下面的式子推出：

$$U_{a,p}=e^{2\pi i\frac{-k\,\mathrm{ind}\,a}{n}}\sum_{x=1}^{p-1}e^{2\pi i\frac{k\,\mathrm{ind}\,ax}{n}}e^{2\pi i\frac{ax}{p}}=e^{2\pi i\frac{-k\,\mathrm{ind}\,a}{n}}U_{1,p}.$$

γ) 明显地，A 和 B 都是整数，并且 $|S|^2=A^2+B^2$。对于某些有条件 $|\varepsilon|=|\varepsilon'|=|\varepsilon''|=1$ 的 $\varepsilon, \varepsilon', \varepsilon''$，我們有(問題 β)

$$S=\frac{1}{\varepsilon\sqrt{p}\,\varepsilon\sqrt{p}}\sum_{z_1=1}^{p-1}\sum_{z=1}^{p-1}\sum_{x=0}^{p-1}e^{-2\pi i\frac{\mathrm{ind}\,z_1+\mathrm{ind}\,z}{4}}e^{2\pi i\frac{z_1x+z(x+1)}{p}}.$$

如果 z_1+z 不等于 p，对 x 求总和給出零。所以

$$S=\varepsilon'\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)e^{2\pi i\frac{z}{p}}=\varepsilon''\sqrt{p},\ |S|^2=p.$$

b, α) 对于給定的 z，同余式 $x^n\equiv z \pmod p$ 只有在 $\mathrm{ind}\,z$ 被 δ 除尽时才能成立，并且那时候这个同余式有 δ 个解答。所以当 $\delta=1$ 时，我們有 $S_{a,p}=0$。而如果 $\delta>1$，則我們有

$$S_{a,p}=1+\sum_{k=0}^{\delta-1}\sum_{z=1}^{p-1}e^{2\pi i\frac{k\,\mathrm{ind}\,z}{\delta}}e^{2\pi i\frac{az}{p}}.$$

当 $k=0$ 时，对 z 求总和給出 -1；当 $k>0$ 时，它的絕对值等于 $\sqrt{p}$。由此推出問題里所說的結果。

β) 假設

$$x=u+p^{s-1}v,\quad u=0,\cdots,p^{s-1}-1,\quad v=0,\cdots,p-1,$$

我們有

$$e^{2\pi i\frac{ax^n}{p^s}}=e^{2\pi ia(u^np^{-s}+nu^{n-1}p^{-1}v)}.$$

当 $(u,p)=1$ 时，对 v 求总和給出零。所以

$$S_{a,p^s}=\sum_{x_0=0}^{p^{s-1}-1}e^{2\pi iap^{n-s}x_0^n}=p^{s-1},\quad S'_{a,p^s}=0.$$

γ) 設 p^τ 是除尽 n 的 p 的最大乘方。我們有 $s\geqslant\tau+3$。假設
$x=u+p^{s-1-\tau}v;\ u=0,\cdots,p^{s-1-\tau}-1,\quad v=0,\cdots,p^{\tau+1}-1,$
我們得出

$$e^{2\pi i\frac{ax^n}{p^s}}=e^{2\pi ia(u^np^{-s}+nu^{n-1}p^{-\tau-1}v)}.$$

当 $(u,p)=1$ 时，对 v 求总和給出零。所以

$$S_{a,p^s}=\sum_{x_0=0}^{p^{s-1}-1}e^{2\pi i\frac{ax_0^n}{p^{s-n}}}=p^{n-1}S_{a,p^{s-n}},\ S'_{a,p^s}=0.$$

δ) 設 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解式，假設

$$T_{a,m}=m^{-1+\nu}S_{a,m};\quad \nu=\frac{1}{n},\quad m=p_1^{\alpha_1}M_1=\cdots=p_k^{\alpha_k}M_k,$$

而且从条件 $a\equiv a_1M_1+\cdots+a_kM_k\pmod m$ 定出 $a_1,\cdots,a_k$，我們有(第三章問題 12, d)

$$T_{a,m}=T_{a_1,p_1^{\alpha_1}}\cdots T_{a_k,p_k^{\alpha_k}}.$$

但是当 $s=1$ 时，我們有

$$|T_{a,p^s}|<p^{-1+\nu}n\sqrt{p}\leqslant np^{-\frac{1}{6}}.$$

当 $1<s\leqslant n$, $(n,p)=1$ 时，我們有

$$|T_{a,p^s}|=p^{-s+s\nu}p^{s-1}\leqslant 1.$$

当 $1<s\leqslant n, (n, p)=p$ 时，我們有

$$|T_{a,p^s}|\leqslant p^{-s+s\nu}p^s\leqslant p\leqslant n.$$

$s>n$ 的情形，由于$T_{a,p^s}=p^{-s+s\nu}p^{n-1}S_{a,p^{s-n}}=T_{a,p^{s-n}}$，可以化成 $s\leqslant n$ 的情形。所以

$$|T_{a,m}|\leqslant C=n^{n^s+n},$$

于是就得出問題里所說的不等式。

12, a. 从問題 11, a, α) 的定理和第五章問題 12, a 的定理推出。

b. 我們有

$$Tn=\sum_{x=M}^{M+Q-1}\sum_{k=0}^{n-1}e^{2\pi i\frac{k(\operatorname{ind}x-s)}{n}}.$$

当 $k=0$ 时，对 x 求总和，我們得到 Q; 当 $k>0$ 时，我們得到的数的絕对值$<\sqrt{p}\ln p$。由此就推出問題里所說的公式。

c. 取 $f(x)=1$ 而且讓 x 通过 $x=\operatorname{ind}M$, $\operatorname{ind}(M+1),\cdots$, $\operatorname{ind}(M+Q-1)$，我們得到 $S'=\sum\limits_{d\diagdown p-1}\mu(d)S_d$(第二章問題 17, a)。这里 S' 是有条件 $(x, p-1)=1$ 的 x 的个数；所以 $S'=T$。再有 S_d 是倍于 d 的 x 的个数，也就是在数列 $M, M+1,\cdots, M+Q-1$ 中 d 次剩余的个数。因此

$$H=\sum_{d\diagdown p-1}\mu(d)\left(\frac{Q}{d}+\theta_d\sqrt{p}\ln p\right);\quad |\theta_d|<1, \theta_1=0.$$

d. 从問題 a 的定理推出，如果讓 $m=p-1$, $\Phi(z)=1$，并且讓 z 通过 $z=\operatorname{ind}x$, $x=M, M+1,\cdots, M+Q-1$，則第五章問題 12, a 的条件都有了。于是我們得到(Q_1 代替 Q)

$$\sum_{z}{}' \Phi(z)=J, \ \sum_{z}\Phi(z)=Q, \ J=\frac{Q_1}{p-1}Q+\theta\sqrt{p}(\ln p)^2.$$

13. 假如沒有不超过 h 的非剩余，則在数 $1, 2, \cdots, [Q]$; $Q=$ $=\sqrt{p}(\ln p)^2$ 中 n 次非剩余的个数可以用兩种方法来估計; 从問題12, b 的公式出發，以及从非剩余只能是被大于 h 的素数除尽的数这事实出發。我們得到

$$1-\frac{1}{n}<\ln\frac{\frac{1}{2}\ln p+2\ln\ln p}{\frac{1}{c}\ln p+2\ln\ln p}+O\left(\frac{1}{\ln p}\right),$$

$$0<\ln\frac{1+4\frac{\ln\ln p}{\ln p}}{1+2c\frac{\ln\ln p}{\ln p}}+O\left(\frac{1}{\ln p}\right).$$

后一不等式不能对于所有充分大的素数 p 都成立，这就証明了定理。

14, a. 我們有

$$|S|^2\leqslant X\sum_{x=0}^{m-1}\sum_{y_1=0}^{m-1}\sum_{y=0}^{m-1}\rho(y_1)\overline{\rho(y)}e^{2\pi i\frac{ax(y_1-y)}{m}}.$$

对于給定的 y_1 和 y，对 x 求总和，給出 $Xm|\rho(y)|^2$ 或者零，就看是否有 $y=y_1$。所以

$$|S|^2\leqslant XYm, \quad |S|\leqslant\sqrt{XYm}.$$

b, α) 我們有

$$S=\frac{1}{\varphi(m)}\sum_{u}\sum_{v}\chi(u)\chi(v)e^{2\pi i\frac{au^nv^n}{m}},$$

这里 u 和 v 都通过与模 m 互素的剩余組。由此

$$S=\frac{1}{\varphi(m)}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\nu(x)\;\rho(y)e^{2\pi i\frac{axy}{m}};$$

$$\nu(x)=\sum_{u^n\equiv x(\bmod m)}\chi(u),\;\rho(y)=\sum_{v^n\equiv y(\bmod m)}\chi(v).$$

但是我們有(第四章問題 11)

$$\sum_{x=0}^{m-1}|\nu(x)|^2\leqslant K\varphi(m),\;\sum_{y=0}^{m-1}|\rho(y)|^2\leqslant K\varphi(m).$$

所以(問題 a)

$$|S|\leqslant\frac{1}{\varphi(m)}\sqrt{K\varphi(m)K\varphi(m)m}=K\sqrt{m}.$$

β) 設 $m=2^\alpha p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解式。同余式 $x^n\equiv1$ $(\bmod m)$ 与下面的組等价:

$$x^n\equiv1(\bmod 2^\alpha),\,x^n\equiv1(\bmod p_1^{\alpha_1}),\,\cdots,\,x^n\equiv1(\bmod p_k^{\alpha_k}).$$

設 $\gamma(x)$ 和 $\gamma_0(x)$ 是 x 对于模 2^α 的指数組(§ 6, g)。同余式 $x^n\equiv1$ $(\bmod 2^\alpha)$ 与組 $n\gamma(x)\equiv0(\bmod c),\,n\gamma_0(x)\equiv0(\bmod c_0)$ 等价。这个組的第一个同余式至多有 2 个解答；第二个至多有 n 个解答。所以同余式 $x^n\equiv1(\bmod 2^\alpha)$ 至多有 $2n$ 个解答。根据 § 5, b，同余式 $x^n\equiv1(\bmod p_1^{\alpha_1}),\,\cdots,\,x^n\equiv1(\bmod p_k^{\alpha_k})$ 的每一个，都至多有 n 个解答。因此

$$K\leqslant2(\tau(m))^{\frac{\ln n}{\ln 2}};\;K=O(m^\varepsilon).$$

15, a. 我們有

$$|S|^2=\sum_{t=1}^{p-1}\sum_{x=1}^{p-1}e^{2\pi i\frac{a(t^n-1)x^n+b(t-1)x}{p}}.$$

如果 $t^n\equiv 1 \pmod p$，則当 $t\equiv 1 \pmod p$ 时，对 x 求总和給出 $p-1$，而在其他的情形則給出 -1。在相反的情形，取 $z(t-1)^{-1}$ 代替 x，这二重的和式中与所取的 t 对应的部分可以表示成

$$\sum_{z=1}^{p-1} e^{2\pi i\frac{bz}{p}} e^{2\pi i\frac{a(t^n-1)(t-1)^{-n}z^n}{p}}.$$

所以

$$|S|^2\leqslant p-1+\left|\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\nu(u)\,\rho(v)e^{2\pi i\frac{auv}{p}}\right|,$$

这里 $\nu(u)$ 等于同余式 $(t^n-1)(t-1)^{-n}\equiv u \pmod p$ 的解答的个数，而且 $|\rho(v)|$ 不超过同余式 $z^n\equiv v \pmod p$ 的解答的个数。所以 $\nu(u)\leqslant 2n_1$, $|\rho(v)|\leqslant n_1$,

$$\sum_{u=1}^{p-1}|\nu(u)|^2\leqslant(p-1)2n_1,\ \sum_{v=1}^{p-1}|\rho(v)|^2\leqslant(p-1)n_1.$$

应用問題 14, a 的定理，我們得到

$$|S|^2\leqslant p-1+\sqrt{(p-1)2n_1(p-1)n_1p}<2n_1p^{\frac{3}{2}}.$$

b, α) 从問題 a 的定理和第五章問題 12, a 的定理推出。

β) 从問題 α 的定理推出，如果讓 $m=p$, $\Phi(z)=1$，并且讓 z 通过 $z=Ax^n, x=M_0, M_0+1, \cdots, M_0+Q_0-1$，則第五章問題 12, a 的条件都有了。所以

$$\sum_z{}' \Phi(z)=T,\quad \sum_z \Phi(z)=Q_0,$$

于是就推出問題里所說的公式。

c, α) 設 $\gamma\equiv 4a\gamma_1 \pmod p$。我們有（第五章問題 11, a）

$$\left(\frac{a}{p}\right)S=\sum_{x=0}^{p-1}\left(\frac{4a^2x^2+4abx+4ac}{p}\right)e^{2\pi i\frac{4a\gamma_1x}{p}}=$$

$$=\frac{1}{U_{1,p}}\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\sum_{x=0}^{p-1}e^{2\pi i\frac{z(4a^2x^2+4abx+4ac+4a\gamma_1xz^{-1})}{p}}=$$

$$=\sum_{z=1}^{p-1}e^{2\pi i\frac{-(b^2-4ac)z-2b\gamma_1-\gamma_1^2z^{-1}}{p}}.$$

最后的和式的值$<\frac{3}{2}p^{\frac{3}{4}}$（問題a）。

β）从問題α的定理和第五章問題12, a 的定理推出。

計算題答案

第一章

1, a. 17。

b. 23。

2, a. α） $\delta_4=\frac{15}{11}$; β） $\alpha=\frac{19}{14}+\frac{\theta}{14\times 20}$。

b. α） $\delta_6=\frac{80}{59}$; β） $\alpha=\frac{1002}{739}+\frac{\theta}{739\times 1000}$。

3. 一共有 22 个分数。

5, a. $2^8\times 3^5\times 11^3$。

b. $2^2\times 3^3\times 5^4\times 7^3\times 11^2\times 17\times 23\times 37$。

第二章

1, a. 13142。

b. $2^{119}\times 3^{59}\times 5^{31}\times 7^{19}\times 11^{12}\times 13^9\times 17^7\times 19^6\times 23^5\times 29^4\times$
$\times 31^4\times 37^3\times 41^3\times 43^2\times 47^2\times 53^2\times 59^2\times 61^2\times 67\times 71\times$
$\times 73\times 79\times 83\times 89\times 97\times 101\times 103\times 107\times 109\times 113$。

2, a. $\tau(5600)=36$; $S(5600)=15624$。

b. $\tau(116\,424)=96$; $S(116\,424)=410\,400$。

3. 所有值的总和等于 1。

4. α） 1152; β） 466400。

5. 所有值的总和等于 774。

第三章

1, a. 70。

b. 能除尽。

2, a. $3^3\times5^2\times11^2\times2999$。

b. $7\times13\times37\times73\times101\times137\times17\times19\times257$。

第四章

1, a. $x\equiv81 \pmod{337}$。

b. $x\equiv200; 751; 1302; 1853; 2404 \pmod{2755}$。

2, b. $x\equiv1630 \pmod{2413}$。

3. $x=94+111t$; $y=39+47t$,这里 t 是整数。

4, a. $x\equiv170\,b_1+52\,b_2 \pmod{221}$; $x\equiv131; 110; 89 \pmod{221}$。

b. $x\equiv11\,151\,b_1+11\,800\,b_2+16\,875\,b_3 \pmod{39\,825}$。

5, a. $x\equiv91 \pmod{120}$。

b. $x\equiv8479 \pmod{15015}$。

6. $x\equiv100 \pmod{143}$; $y\equiv111 \pmod{143}$。

7, a. $3x^4+2x^3+3x^2+2x\equiv0 \pmod 5$。

b. $x^5+5x^4+3x^2+3x+2\equiv0 \pmod 7$。

8. $x^6+4x^5+22x^4+76x^3+70x^2+52x+39\equiv0 \pmod{101}$。

9, a. $x\equiv16 \pmod{27}$。

b. $x\equiv22;\ 53 \pmod{64}$。

10, a. $x\equiv113 \pmod{125}$。

b. $x\equiv43,\ 123,\ 168,\ 248,\ 293,\ 373,\ 418,\ 498,\ 543,\ 623 \pmod{625}$。

11, a. $x\equiv2, 5, 11, 17, 20, 26 \pmod{30}$。

b. $x\equiv76, 22, 176, 122 \pmod{225}$。

第五章

1, a. 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18。

b. 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35。

2, a. α) 0; β) 2。

b. α) 0; β) 2。

3, a. α) 0; β) 2。

b. α) 0; β) 2。

4, a. α) $x\equiv\pm 9 \pmod{19}$; β) $x\equiv\pm 11 \pmod{29}$;

γ) $x\equiv\pm 14 \pmod{97}$。

b. α) $x\equiv\pm 66 \pmod{311}$; β) $x\equiv\pm 130 \pmod{277}$;

γ) $x=\pm 94 \pmod{353}$。

5, a. $x\equiv\pm 72 \pmod{125}$。

b. $x\equiv\pm 127 \pmod{243}$。

6, a. $x\equiv 13, 19, 45, 51, \pmod{64}$。

b. $x\equiv 41, 87, 169, 215 \pmod{256}$。

第六章

1, a. 6。

b. 18。

2, a. 3, 3, 3。

b. 5, 5, 5。

c. 7。

5, a. α) 0; β) 1; γ) 3。

b. α) 0; β) 1; γ) 10。

6, a. α) $x\equiv 40, 27 \pmod{67}$; β) $x\equiv 33 \pmod{67}$;

γ) $x\equiv 8, 36, 28, 59, 31, 39 \pmod{67}$。

b. α) $x\equiv 17 \pmod{73}$; β) $x\equiv 50, 12, 35, 23, 61, 38 \pmod{73}$; γ) $x\equiv 3, 24, 46 \pmod{73}$。

7, a. α) 0; β) 4。

b. α) 0; β) 7。

8, a. α) $x \equiv 54 \pmod{101}$; β) $x \equiv 53, 86, 90, 66, 8 \pmod{101}$。

b. $x \equiv 59, 11, 39 \pmod{109}$。

9, a. α) 1, 4, 5, 6, 7, 9, 11, 16, 17; β) 1, 7, 8, 11, 12, 18。

b. α) 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36; β) 1, 7, 9, 10, 12, 16, 26, 33, 34。

10, a. α) 7, 37; β) 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34。

b. α) 3, 27, 41, 52; β) 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59。

指　数　表

素　数　3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

素　数　5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

素　数　7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

素　数　11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

素　数　13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

素 数 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

素 数 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

素 数 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

素 数 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

素 数 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

素 数 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

素 数 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

素 数 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

素 数 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

素 数 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

素 数 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

素 数 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	4.	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

素 数 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

素 数 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	43	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

素 数 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

素 数 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

素 数 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

素 数 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

素 数 97

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	6	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	8	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

4000 以下的素数和它們的最小元根表

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

繼續前面

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2129	3	2417	3	2729	3	3049	11	3373	5	3691	2
1831	3	2131	2	2423	5	2731	3	3061	6	3389	3	3697	5
1847	5	2137	10	2437	2	2741	2	3067	2	3391	3	3701	2
1861	2	2141	2	2441	6	2749	6	3079	6	3407	5	3709	2
1867	2	2143	3	2447	5	2753	3	3083	2	3413	2	3719	7
1871	14	2153	3	2459	2	2767	3	3089	3	3433	5	3727	3
1873	10	2161	23	2467	2	2777	3	3109	6	3449	3	3733	2
1877	2	2179	7	2473	5	2789	2	3119	7	3457	7	3739	7
1879	6	2203	5	2477	2	2791	6	3121	7	3461	2	3761	3
1889	3	2207	5	2503	3	2797	2	3137	3	3463	3	3767	5
1901	2	2213	2	2521	17	2801	3	3163	3	3467	2	3769	7
1907	2	2221	2	2531	2	2803	2	3167	5	3469	2	3779	2
1913	3	2237	2	2539	2	2819	2	3169	7	3491	2	3793	5
1931	2	2239	3	2543	5	2833	5	3181	7	3499	2	3797	2
1933	5	2243	2	2549	2	2837	2	3187	2	3511	7	3803	2
1949	2	2251	7	2551	6	2843	2	3191	11	3517	2	3821	3
1951	3	2267	2	2557	2	2851	2	3203	2	3527	5	3823	3
1973	2	2269	2	2579	2	2857	11	3209	3	3529	17	3833	3
1979	2	2273	3	2591	7	2861	2	3217	5	3533	2	3847	5
1987	2	2281	7	2593	7	2879	7	3221	10	3539	2	3851	2
1993	5	2287	19	2609	3	2887	5	3229	6	3541	7	3853	2
1997	2	2293	2	2617	5	2897	3	3251	6	3547	2	3863	5
1999	3	2297	5	2621	2	2903	5	3253	2	3557	2	3877	2
2003	5	2309	2	2633	3	2909	2	3257	3	3559	3	3881	13
2011	3	2311	3	2647	3	2917	5	3259	3	3571	2	3889	11
2017	5	2333	2	2657	3	2927	5	3271	3	3581	2	3907	2
2027	2	2339	2	2659	2	2939	2	3299	2	3583	3	3911	13
2029	2	2341	7	2663	5	2953	13	3301	6	3593	3	3917	2
2039	7	2347	3	2671	7	2957	2	3307	2	3607	5	3919	3
2053	2	2351	13	2677	2	2963	2	3313	10	3613	2	3923	2
2063	5	2357	2	2683	2	2969	3	3319	6	3617	3	3929	3
2069	2	2371	2	2687	5	2971	10	3323	2	3623	5	3931	2
2081	3	2377	5	2689	19	2999	17	3329	3	3631	21	3943	3
2083	2	2381	3	2693	2	3001	14	3331	3	3637	2	3947	2
2087	5	2383	5	2699	2	3011	2	3343	5	3643	2	3967	6
2089	7	2389	2	2707	2	3019	2	3347	2	3659	2	3989	2
2099	2	2393	3	2711	7	3023	5	3359	11	3671	13		
2111	7	2399	11	2713	5	3037	2	3361	22	3673	5		
2113	5	2411	6	2719	3	3041	3	3371	2	3677	2		

中文、俄文、英文名詞对照表

个数	число	number
与模互素的剩余組	приведённая система вычетов	set of residues prime to the modulus
牛頓二項式	бином Ньютона	Newton's binomial
不等式	неравенство	inequality
互素的	взаимно простой	relatively prime
兩兩 ～	попарно простой	pairly ～
分子	числитель	numerator
分母	знаменатель	denominator
分解式	разложение	decomposition (or factorization)
标准 ～	каноническое ～	canonical ～
分数	дробь	fraction
近似 ～	подходящяя ～	approximate ～
不可約 ～	несократимая ～	irreducible ～
分数部分	дробная часть	fractional part
方次数	показатель	exponent
方程	уравнение	equation
不定 ～	неопределённое ～	indeterminate ～
比率	отношение	ratio
号碼	номер	number
对数	логарифм	logarithm
对应	отвечанщий	correspondent
可除性	делимость	divicibility
可能率	вероятность	probability
平方	квадрат	square
平方剩余	квадратичный вычет	quadratic residue
平方非剩余	квадратичный невычет	quadratic non-residue
必要性	необходимость	necessity
未知数	неизвестный	unknown
正的	положительный	positive

立方的	кубический	cubic
充分性	достаточность	sufficiency
共軛的	сопряжённый	conjugate
次数	степень	degree
同余式的 ～	～ сравнения	～ of congruence
同余式	сравнение	congruence
因子	сомножитель	factor
素 ～	простой ～	prime ～
多項式	многочлен	polynomial
收斂的	сходищийся	convergent
有上界	ограниченный сверху	bounded above
有理数	рациональное (число)	rational (number)
自然数	натуральное число	natural number
导数	производная	derivative
二阶 ～	вторая ～	second ～
弗尔馬定理	теорема Ферма	Fermat's theorem
余数	остаток	remainder
坐标	координата	coordinate
系数	коэффициент	coefficient
完全剩余組	полная система вычетов	complete set of residues
函数	функция	function
可乘 ～	мультипликативная ～	multiplicative ～
有理 ～	рациональная ～	rational ～
沛勒方程	уравнение Пелля	Pell's equation
法雷級数	ряд Фарея	Farey's series
和数(和式,总和)	сумма	sum
奇数	нечётное (число)	odd (number)
运算	операция	operation
实数	вещественное (число)	real (number)
表示式	выражение	expression
复合数	составное (число)	composite
复数	комплексное число	complex number
总和	сумма	sum
求 ～	суммирование	summation
品格	характер	character
主 ～	главный ～	principal ～
恒等式	тождество	identity
指数	индекс	index

界限	граница	bound
約数	делитель	divisor
公 ~	общий ~	common ~
最大公 ~	общий наибольший ~	greatest common ~
負的	отрицательный	negative
非 ~	не~	non~
欧拉定理	теорема Эйлера	Euler's theorem
欧拉函数	функция Эйлера	Euler's function
欧拉常数	постоянная Эйлера	Euler's constant
欧几里得算法	алгоритма Эвклида	Euclidean algorithm
茂陛烏斯函数	функция Мёбиуса	Möbius' function
威尔遜定理	теорема Вильсона	Wilson's theorem
乘方数	степень целого	integral power
乘积	произведение	product
倍数	кратное	multiple
公 ~	общее ~	common ~
最小公 ~	общее наименьшее ~	least common ~
根	корень	root
元 ~	первообразный ~	primitive ~
級数	ряд	series
調和 ~	гармонический ~	harmonical ~
素数	простое (число)	prime (number)
差数	разность	difference
除尽	делить	devide
积分	интегрирование	integration
泰乐公式	формула Тейлора	Taylor's formula
爱拉托散的篩子	решето Эратосфена	the sieve of Eratosthenes
值	значение	value
商数	частное	quotient
不完全 ~	неполное ~	incomplete ~
常数	постоянная	constant
連分式	непрерывная дробь	continued fraction
連續的	непрерывный	continuous
頂点	вершина	vertex
偶数	чётное (число)	even (number)
梭宁公式	формула Сонина	Sonin's formula
勒祥得尔符号	символ Лежандра	Legendre's symbol
剩余	вычет	residue

非～	не～	non～
最小 ～	наименьший ～	least ～
～ 集合	～ класс (вычетов)	～ residue class
極限	предел	limit
無理数	иррациональное (число)	irrational (number)
發散的	расходящийся	divergent
等式	равенство	equality
等价	равносильный	equivalent
絕对的	абсолютный	absolute
絕对值	модуль	absolute value
間隔	интервал	interval
集合	совокупность, класс	set; class
項	член	term
雅可比符号	символ Якоби	Jacobi's symbol
解答	решение	solution
零	нуль	zero (or null)
数	число	number
数列	ряд	sequence
数論	теория чисел	theory of numbers
模	модуль	modulus
整数	целое (число)	integer
正 ～	положительное ～	positive ～
負 ～	отрицательное ～	negative ～
整数部分	целая часть	integral part
整点	целая точка	integral point